A3

2/5/1 (Item 1 from file: 351)
DIALOG(R)File 351:Derwent WPI

011045987 **Image available**
WPI Acc No: 1997-023911/199703
Related WPI Acc No: 1995-264029; 1999-142307; 1999-613171

Digital signing method esp. for high value documents - using several separate signing devices containing partial signatures which are each associated with authorising agent to affix or modify partial signature

Patent Assignee: CERTCO LLC (CERT-N); BANKERS TRUST CO (BANK-N); CERTCO INC (CERT-N); BANKERS TRUST COMP (BANK-N); FREUND P C (FREU-I); HUANG S T F (HUAN-I); SUDIA F W (SUDI-I)
Inventor: FREUND P C; HUANG S T F; SUDIA F W; FREUND P; HUANG S; SUDIA F; HUANG S T; SUDLA F W
Number of Countries: 074 Number of Patents: 017
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
GB 2301919	A	19961218	GB 9610291	A	19960516	199703	B
WO 9639765	A1	19961212	WO 96US5317	A	19960419	199704	
ZA 9603635	A	19970129	ZA 963635	A	19960508	199710	
AU 9655521	A	19961224	AU 9655521	A	19960419	199715	
TW 307075	A	19970601	TW 96105565	A	19960510	199737	
EP 872080	A1	19981021	EP 96912843	A	19960419	199846	
			WO 96US5317	A	19960419		
US 5825880	A	19981020	US 94181859	A	19940113	199849	
			US 94272203	A	19940708		
			US 95462430	A	19950605		
			US 97869253	A	19970604		
BR 9608416	A	19981229	BR 968416	A	19960419	199909	
			WO 96US5317	A	19960419		
JP 11506222	W	19990602	WO 96US5317	A	19960419	199932	
			JP 97500473	A	19960419		
GB 2301919	B	20000301	GB 9610291	A	19960516	200014	
GB 2337145	B	20000301	GB 9610291	A	19960516	200014	
			GB 9918950	A	19990811		
MX 9709760	A1	19980801	MX 979760	A	19971205	200014	
NZ 306846	A	20000128	NZ 306846	A	19960419	200015	
			WO 96US5317	A	19960419		
KR 99022451	A	19990325	WO 96US5317	A	19960419	200023	
			KR 97708932	A	19971205		
IL 118363	A	20000217	IL 118363	A	19960522	200027	
AU 718265	B	20000413	AU 9655521	A	19960419	200028	
CN 1192834	A	19980909	CN 96196055	A	19960419	200040	

Priority Applications (No Type Date): US 95462430 A 19950605; US 94181859 A 19940113; US 94272203 A 19940708; US 97869253 A 19970604
Cited Patents: US 5005200; US 5164988; US 5224163; US 5276737; US 5481613
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
GB 2301919	A		81	H04L-009/32	
WO 9639765	A1	E	80	H04L-009/30	
Designated States (National): AL AM AT AU AZ BB BG BR BY CA CH CN CZ DE DK EE ES FI GB GE HU IS JP KE KG KP KR KZ LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK TJ TM TR TT UA UG US UZ VN					
Designated States (Regional): AT BE CH DE DK EA ES FI FR GB GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG					
ZA 9603635	A		81	G09C-000/00	
AU 9655521	A			H04L-009/30	Based on patent WO 9639765
TW 307075	A			H04J-009/28	
EP 872080	A1	E		H04L-009/30	Based on patent WO 9639765
Designated States (Regional): AT CH DE ES FR GB IE IT LI					
US 5825880	A				CIP of application US 94181859 CIP of application US 94272203 Cont of application US 95462430
BR 9608416	A			H04L-009/30	Based on patent WO 9639765
JP 11506222	W		95	G09C-001/00	Based on patent WO 9639765
GB 2301919	B			H04L-009/32	
GB 2337145	B			H04L-009/32	Derived from application GB 9610291

MX 9709760	A1	H04L-009/30	
NZ 306846	A	H04L-009/30	Based on patent WO 9639765
KR 99022451	A	H04L-009/30	Based on patent WO 9639765
IL 118363	A	H04L-009/32	
AU 718265	B	H04L-009/30	Previous Publ. patent AU 9655521 Based on patent WO 9639765
CN 1192834	A	H04L-009/30	

Abstract (Basic): GB 2301919 A

The method generates shares of a private signature and stores them in separate electronic signing devices. Each signing device comprises an electronic device which is programmed to receive an electronic document. The method then certifies multiple authorising agents for the signing devices. Each agent comprises an electronic device which is programmed to provide an authorisation to an associated signing device.

For each signing device, a partial signature is affixed to an electronic message in response to authorisation from a minimum number of authorising agents. The final digital signature is made up of several partial signatures. Pref. the method arranges the signing devices as a system of interlocked rings. The signing devices are split into two groups where the first includes at least one member which is not in the second and the first also includes one common member.

USE/ADVANTAGE - E.g for certificates and other high value documents e.g. contracts, negotiable documents or electronic representations of currency. No single signing device contains signature key during document signing operation. Permits loss or compromise of one or more signing devices while maintaining available un-compromised signing services. Uses multiple signing devices in conjunction with authorising devices to produce single digital signature. Robust and easy-to-use.

Dwg.1/25

Title Terms: DIGITAL; SIGN; METHOD; HIGH; VALUE; DOCUMENT; SEPARATE; SIGN; DEVICE; CONTAIN; SIGNATURE; ASSOCIATE; AUTHORISE; AGENT; AFFIX; MODIFIED; SIGNATURE

Derwent Class: P85; W01

International Patent Class (Main): G09C-000/00; G09C-001/00; H04J-009/28; H04L-009/30; H04L-009/32

International Patent Class (Additional): H04K-000/00; H04L-029/06

File Segment: EPI; EngPI

(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号

特表平11－506222

(43)公表日　平成11年(1999)６月２日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｂ
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｂ
			６７５Ｄ

審査請求　未請求　予備審査請求　有　（全 95 頁）

(21)出願番号　特願平9－500473
(86)(22)出願日　平成８年(1996)４月19日
(85)翻訳文提出日　平成９年(1997)12月５日
(86)国際出願番号　ＰＣＴ／ＵＳ９６／０５３１７
(87)国際公開番号　ＷＯ９６／３９７６５
(87)国際公開日　平成８年(1996)12月12日
(31)優先権主張番号　０８／４６２，４３０
(32)優先日　1995年６月５日
(33)優先権主張国　米国（ＵＳ）

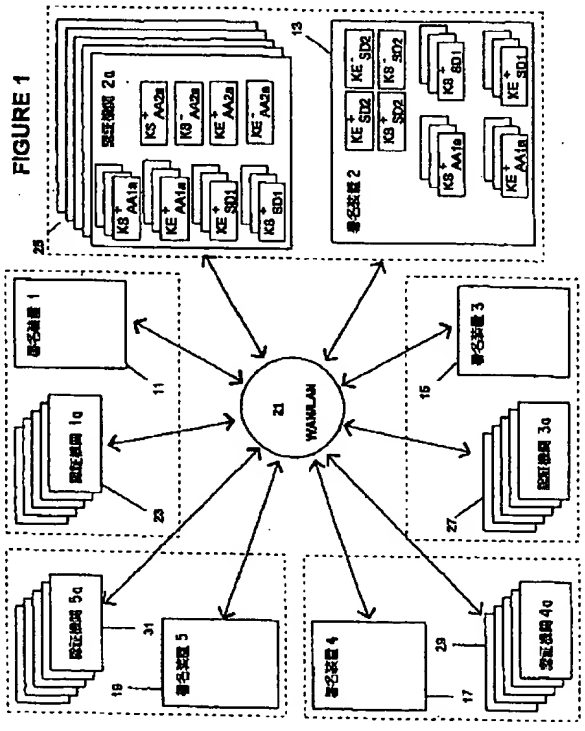
(71)出願人　サートコー・エルエルシー
アメリカ合衆国、ニューヨーク州　10017、ニューヨーク、パーク・アベニュー　280
(72)発明者　スーディア、フランク・ダブリュ
アメリカ合衆国、マサチューセッツ州　02195、ニュートン・センター、ウォーレン・テラス　４
(72)発明者　フロイント、ピーター・シー
アメリカ合衆国、ニューヨーク州　10021、ニューヨーク、イースト・セブンティーナインス・ストリート　139、エイス・フロアー
(74)代理人　弁理士　鈴江　武彦　（外４名）

最終頁に続く

(54)【発明の名称】　マルチステップディジタル署名方法およびそのシステム

(57)【要約】
多数の署名装置（１１、１３、１５、１７、１９）を用いるマルチステップ署名システム及び方法は単一の公開照合鍵をもちいて照合される単一の署名を添付する。各署名装置は署名鍵の部分を有し、多数の認証機関（２３、２５、２７、２９、３１）からの認証に応じて部分的な署名を添付する。シリアルな実施例では第１の部分署名が添付された後、第２の署名装置が第１の部分署名を累乗する。パラレルな実施例では、各署名装置は部分署名を添付し、多数の部分署名は最終的な署名を形成するために掛け合わされる。多数の署名装置の間で部分署名を添付する能力を分配すること、及び多数の認証機関の間で部分署名を添付する権限を分配することによりシステムのセキュリティは向上される。

FIGURE 1



【特許請求の範囲】

１．秘密署名鍵の部分を作成するステップと、

別個の電子署名装置へ部分を保存するステップと、

署名装置の複数の認証機関を認証するステップと、

複数の署名装置のそれぞれにおいて、最低数の認証機関からの認証に応じて電子メッセージに部分署名を添付するステップとを具備し、

複数の部分署名によってディジタル署名が構成されるディジタル署名方法。

２．ディジタル署名を電子文書に添付するシステムであって、

電子文書を受け取り、予め決められた数の認証に応じて、署名鍵部分を用いて部分署名を添付するようにプログラミングされている電子装置からなる複数の相互通信署名装置と、

関連の署名装置と通信でき、関連の署名装置に認証を提供するようにプログラミングされている電子装置からなる複数の認証機関とを具備するシステム。

３．電子文書にディジタル署名を添付するための署名装置のインターロックリングシステムであって、

複数の電子装置を含んでおり、それぞれの装置は、電子文書を受け取り、最初の署名鍵に部分署名を添付するようにプログラミングされ、この複数の部分署名は最初のディジタル署名を含んでいる、署名装置の第１集合と、

複数の電子装置を具備し、各装置は、電子文書を受け取り、第２署名鍵のために部分署名を添付するようにプログラミングされ、この複数の部分署名は２番目のディジタル署名を含んでいる、署名装置の第２集合とを具備し、

前記第１は、前記第２集合には含まれないメンバーを少なくとも１つは含み、第１集合と第２集合は少なくとも１つの共通メンバーを含むシステム。

４．最初の電子装置に鍵を保存するステップと、

代理人に電子委任証明書を送るステップと、

代理人から最初の電子装置に要求と委任証明書を送るステップと、

最初の電子装置を用いて、要求と委任証明書に応じて電子鍵を使用するステップとを具備する電子鍵の代理使用のための電子的方法。

【発明の詳細な説明】

マルチステップディジタル署名方法およびそのシステム

本出願は、米国特許出願第０８／１８１，８５９号「鍵寄託機能を伴う暗号化システム」及び米国特許出願第０８／２７２，２０３号「鍵寄託機能を伴う高度な暗号化のシステムと方法」の一部継続出願であって、これらは本明細書に参考として組み込まれる。

背景技術

公開鍵証明書とは、信用発行者が署名し、ユーザ名と公開鍵またはその他の関連データとの結合を証明するのに使用される電子文書である。証明書は、証明書で識別された公開鍵が、証明書に名前が記載されているユーザによって所有されていることを公に保証する。公開鍵証明システムを記述している主な標準には、ITU-T X.509 The Directory - Authentication Framework, American Bankers Association ANSI X9.30 - Part 3, Certificate Management for DSA(draft)などがある。多数の実施例は、保証認証機関（ＣＡ）として参照される各信用発行者が下位の法人の鍵を証明する階層構造をなしている。ＣＡは、証明可能で（ＣＡが文書に署名したことを証明できる）、偽造不可能な（ＣＡ以外のものが文書に署名していないという高度な信頼性を保証する）方法で、電子文書にディジタル署名を添付する。例えば、ＣＡ階層の最上位には、おそらく下位レベルのＣＡを証明する国ごとに１つの、比較的少ないルート（基幹）ＣＡが存在しうる。階層においてＣＡの下には、高レベルのＣＡ（おそらく銀行）がその下の下位レベルのＣＡ（例えば、会社）を証明し、さらにこのＣＡが個別ユーザ証明書に署名する。

ＣＡの署名は、その下のユーザからなる大きな階層を作成し、高価値のユーザおよび下位のＣＡの両方の証明書に署名するのに署名鍵を使うにつれて、より価値の高いものになる。したがって、ＣＡの署名鍵は、テロリストや不正な経済的利益の求める犯罪者、さらに経済的スパイや情報戦争によって経済の不安定化を狙っている外国の軍隊やスパイ組織の標的になる。これらの問題は、電子貨幣に署名するのに使われる鍵にも等しく当てはまる。

これまで、ＣＡの秘密署名鍵のセキュリティに対するニーズは、証明書署名装

置（certificate signing unit：ＣＳＵ）を提供することにより取り組まれてきた。このＣＳＵとは、米国商務省のNational Institute of Standards and Technology（ＮＩＳＴ）が発行した連邦情報処理標準（Federal Information Processing Standard：ＦＩＰＳ）PUB 140-1，レベル３またはレベル４に規定されている基準を満たす変造不可能で信頼性の高いモジュールである。このＣＳＵは、公開／秘密署名鍵の仕組を内的に作成し、秘密署名鍵を確実にまた永久的に、外部から読み取り不可能で、その署名を確認するのに使われる対応の公開鍵だけを出力するデバイスのエリア内部に封じ込める。Boston，MAのBolt，Barenek，Newton（ＢＢＮ）から利用できる１つのＣＳＵは、その秘密署名鍵のバックアップによって「Ｋ－ｏｆ－Ｎ閾値」方式を用いた作成を許可するよう構成されている。この「Ｋ－ｏｆ－Ｎ閾値」方式では、秘密鍵はＮ個の部分に分割されて、それぞれがメモリチップを含んでいる小さなプラスチックデータキーに入れられる。データキーは、Burnsville，MNのDetakey，Inc.社の特許製品である。ＣＳＵが万一破壊されても、少なくともＫ個のデータキーの過半数は、秘密鍵を復元しうる。

少なくとも１つの主要なセキュリティ標準化団体、すなわち大規模銀行における暗号化セキュリティを扱っているAmerican Bankers Association ANSI X9.F1委員会は、鍵の窃盗や不正使用を防止するために、ＣＰＵはいかなる形でもデバイスからの秘密鍵の持ち出しを禁ずるように設計されるべきであると勧告している。このやり方では、鍵の複数の対の同時使用を含む、災害復旧のための優れた手順が必要になる。１つの鍵は、１つのサイトの１つのＣＳＵにだけ存在するので、ＣＳＵまたはサイトが喪失した場合、事業を継続するためには別の鍵の対を使わなければならない。これにより、ＣＡは、それぞれ異なるコード番号（例えば、ＢＴ０１、ＢＴ０２、ＢＴ０３）によって識別される複数の（少なくとも２または３の）公開鍵を発行及び／又は配布することを求めている。このようにして、ユーザは、ＢＴ０１の秘密鍵を含んでいる１つのＣＳＵが破壊された後にＣＡが発行する署名を確認することができる。災害復旧の手順については、X9.30 - Part３を参照。

発明の開示

本発明の目的は、証明書や、契約書、電子通貨、契約文書等の他の貴重な文書のために、安全性と柔軟性が高いディジタル署名システム（以後署名システムと略す）を提供することである。

本発明のさらなる目的は、署名システムと署名鍵との間の関係が証明可能であり、いかなる署名装置も文書署名実行時に署名鍵を含む必要がないような署名システムを提供することである。

本発明の他の目的は、利用可能な安全な署名サービスの保守時に１つまたは複数の署名装置の喪失または安全性の低下を許すような署名システムの提供することである。

本発明の別の目的は、複数の署名装置がそれぞれ１つまたは複数の部分署名を作成、変更、結合でき、複数の署名装置による処理の結果１つのディジタル署名が作成されるような署名システムを提供することである。

本発明の別の目的は、各署名装置が部分署名を添付あるいは変更することを複数の認証機関が直接、間接に認める署名システムを提供することである。

本発明のさらに別の目的は、認証機関が一時的にその許可権限を委任できる強固で使い易い機構を提供することである。

ここで説明するマルチステップ署名システムは、文書の受領者が署名者の公開照合鍵を用いて署名を確認できるように、公開鍵暗号システム方式を用いて電子文書に署名する。公開照合鍵に対応する秘密照合鍵は、通常の署名作業時には、絶対に１つの場所にいかなる形でも存在することは許されない。その代りに、秘密署名鍵は、部分署名を添付または変更するのに使うことができるオペレーショナルシェア（機能部分）から構成される。複数の部分の順次処理により、公開鍵を用いて確認できる署名が作成される。完全署名は、署名装置のすべてまたはいくつかが署名し終るまで完了しない。また、各署名装置は、署名プロセスに参加する前に、すべての、またはいくつかの関連認証機関らの許可を必要とする。

機能部分の初期作成時に、署名鍵全体が作成される場合、機能部分が配布された後にその署名鍵全体が破壊される。ある装置の盗難または故障による喪失の危険が大幅に減少するので、いかなる装置が故障しても、簡単に交換（または、再構築）し、サービスを再開して、（例えば、リモートバックアップや、プラグイ

ン交換またはホットスタンバイなどのために）各署名装置の情報内容を複製できる。署名処理は１つの装置では完結しないので、個別署名装置の破壊の影響が低下する。

多層構成の認証管理システムが確立され、各署名装置はその中に多数の個人（または、指定の個人が使う外部スマートカード）を登録し、署名装置は、過半数の登録個人からの許可にのみ基づいて署名活動に参加する。認証機関と呼ばれる過半数の登録個人も、追加認証機関の登録、認証機関の削除、署名装置が実行しうる様々なアクションに対する過半数要件の変更、または追加または代わりの鍵の対の作成や配布のような、システムに対する変更を許可することが求められる。

このようにして、公開照合鍵を用いて検証される署名が通用できるが、いかなる秘密署名鍵も、危険または災害の恐れのある一箇所には存在しない。署名サービスを中断する前に、または敵対者が署名を捏造するのに十分な情報を得る前に、複数のサイトがダウンしなければならない。個別署名装置は、１つの全体鍵を使うＣＳＵほど高度な安全性は求められない。FIPS 140-1 レベル３の基準を満たす比較的安価な装置、すなわち、干渉に強い装置を使うことができるので、変造が検出されたときに内部情報の破壊または保護に積極的な対策を必要とする比較的高価なレベル４装置を使わなくてもすむ。

権限委任機構により、認証機関は、一人の代理人または過半数の代理人が署名を添付することを、一時的に自分のスマートカードが認めるようにすることができる。

図面の簡単な説明

本発明は、以下のような添付図面を参照しながら説明される。

図１は本発明に従った署名システムの基本構造の概要を示す。

図２は署名装置を持っているデータセンターの好ましい構造を示す。

図３は認証機関が使う信用装置の好ましい構造を示す。

図４はシステム開始時および初期化時において、一時的に新参の署名装置を認証するプロセスを示す。

図５はシステム全体で有効な鍵のオペレーショナルシェアを作成し、配布する

プロセスを示す。

図６は署名装置を再認証するためのマルチステップ署名手順を示す。

図７は認証機関を認証し登録するためのシステム構造全体を示す。

図８は認証機関を使ったマルチステップ署名手順を示す。

図９は定型的なマルチステップ署名処理時に様々な認証機関や署名装置を通る文書の流れを示す。

図１０は定型的なマルチステップ署名処理時における文書に対する署名の進展を示す。

発明を実施するための最良の形態

先ず、いくつかの計算プロセスから始めて、マルチステップ署名方法を最も直截に説明する。

A．順次部分署名における乗法方式

最初に、システム全体で有効な権限に属する公開／秘密鍵の対の秘密署名鍵K_{SAW}は、署名鍵K_{SWA}が部分の閾値ｔ０の積として計算できるように、部分a_iの数ｎ０として表される。ここで、ｔ０はｎ０に等しいか、それ以下である。このように表されるので、ｔ０より少ない部分を処理しても、署名鍵K_{SWA}を回復することは極めて困難である。例えば、これは以下の、１）Shamir式の秘密共用方式を使う、(A. Shamir, " How to Share a Secret", Communications of the ACM, Nov. 1979, V. 22, n.11)、２）Blakey式の秘密共用方式を使う(G. R. Blakley, "Safeguarding Cryptographic keys", Proceedings of the National Computer Conference, 1979, American Federation of Information Processing Societies, V.48, 1979, pp. 242-268)、３）鍵を因数分解する、４）既知の因数の積として鍵を作成することにより実行できる。必要なことは、秘密鍵が以下のように表わされることだけである。

$K^{-}_{SWA} = a_1 * a_2 * \ldots * a_{t0} \pmod{2N}$

ここで、K_{SWA}は、署名鍵であり、a_iはｔ０部分の組み合わせである。

第２に、各装置に前の装置が残した部分署名を累乗させることにより複数の装置を用いて、また秘密鍵の１つの部分を用いて、署名が作成される。法Ｎを使う

場合（ここでは、演算は、法Ｎによって結果を割り、剰余を法Ｎの結果として取ることにより終る）、指数の乗算と順次累乗の間の以下の関係が真になる：

$(X^{a1*a2})(\mathrm{mod}\ N)=((X^{a1})^{a2})(\mathrm{mod}\ N)=((X^{a2})^{a1})(\mathrm{mod}\ N)$

言い換えれば、ベース値ｘが２つの因数ａ１とａ２の積によって累乗されると、ベースが最初の因数ａ１によって累乗され、その結果が２番目の因数ａ２によって累乗されたかのように、結果は同じになる。さらに、累乗の順序を反転することができる。それにより、最初にベースが２番目の因数ａ２によって累乗され、その結果が最初の因数ａ１によって累乗されたのと同じ結果になる。この関係は、３以上の因数による累乗に一般化することができる。特に明記しない場合、すべての演算は、法Ｎと見なされなければならない。

マルチステップ署名方式では、署名鍵a_1，a_2，．．．，a_{n0}の部分は別個の装置に配布される。最初の装置は、文書をハッシングし、以下のようなハッシュ(Hash)関数を累乗して文書に部分署名を添付する（記号Ｈは、ハッシュ演算の結果を示すのに使われている）。

最初の部分署名 ＝ $(H)^{a1}(\mathrm{mod}\ N)$

２番目の装置は、以下のように２番目の部分a_2を用いて、最初の部分署名を累乗して追加署名を行なう。

２番目の部分署名 ＝ $((H^{a1}))^{a2}(\mathrm{mod}\ N)$

ｔ０装置がそれぞれのｔ０部分を用いてハッシュを累乗し、公開鍵K^{-}_{SWA}を用いて認証できる最終署名を作成するまで、このプロセスが繰り返される。

Ｂ．非同期的部分署名での加算方式

同じような結果を得るための代替方式では、署名権限者の秘密鍵を、法Ｎで加算して、秘密鍵を作成できるような部分に分割する。

$K=a_1+a_2+\ldots a_t(\mathrm{mod}\ N)$

これによって、以下に示すように、ハッシュを各部分で累乗しその結果を掛けて、別個に中間値$(H)^{ai}$を得て、非同期的にマルチステップ署名を実行することができるようになる。

$S=H^{a1}*H^{a2}*\ldots H^{a3}(\mathrm{mod}\ N)$

これは、メッセージをある位置から別の位置に順次ルーティングする必要がな

いので、先に説明した順次法よりも、処理面でかなり有利である。その代わりに、中央の管理者は、部分署名を求めて、同じメッセージ（または、ハッシュ）を直接に各位置に送り、その部分署名を結合して、最終の正式署名を作成することができる。部分署名にまだ含まれていない情報を追加することはないので、この最終結合処理は特別のセキュリティを必要としない。したがって、管理者はデスクトップから作業することができる。確かに、取り引きを検証する受領者が、部分署名を後で結合するという作業を行わなければならないが、これにより正式署名のセキュリティが弱まることはない。

マルチステップ署名を行えるように変更できる累乗に基づいた署名方式には、以下のものがある。R. Rivest, A. Shamir and L. Adleman（ＲＳＡ），「ディジタル署名と公開鍵暗号化システムを得るための方法」，Communications of the ACM, v.21, n.2, pp.120-126, February 1978)；D. Kravitz, Digital Signature algorithm（ＤＳＡ），U.S. Patent No. 5,231,668; Desmet, Y. Frankel,「閾値暗号化システム」，CRYPTO, '89, pp.307-15, 1989: Taher El-Gamal,「離散化アルゴリズムに基づいた公開鍵暗号化システムと署名方式」，（"El-Gamal Signature Algorithm"），IEEE Transaction on Information Theory, Vol. IT-31, No.4, Jul. 1985; S. Micali「安全で効率的なディジタル署名システム」，MIT／LCS／TM-501, Massachusetts Institute of Technology, laborator for Computer Science, March 1994; A. Menezes et al.,「楕円曲線公開鍵暗号化システム」，1993。

システム概要

図１は、本発明に従った署名システムの構造の概要を示している。この構造は、広域ネットワーク（ＷＡＮ）またはローカルエリアネットワーク（ＬＡＮ）２１によって相互に接続された複数の署名装置１１，１３，１５，１７，１９を含んでいる。個々の署名装置１１，１３，１５，１７，１９は、ＷＡＮ／ＬＡＮが許す限り、地理的にいかなる範囲にでも分散させることができる（複数の大陸、複数の都市、１つの都市の複数の地域）。

図１には、署名装置２が、例として詳細に示されている。各署名装置には、通

信の暗号化／復号化のために、公開／秘密鍵の対１２ａ，１２ｂと並んで、恒久的な識別コード（例えば、ユニークなシリアル番号）と論理名（例えば、署名装置Ｘ）が、また署名の認証と実行のために別個の公開／秘密鍵の対１４ａ，１４ｂが割り当てられる。さらに、各署名装置は、他の署名装置のために公開暗号化鍵１６と公開認証鍵１８を受け取る。

以後、署名／認証鍵はＫＳとして指定され、暗号化／復号化鍵はＫＥとして指定される。プラス（＋）の上付き文字は公開鍵を示し、マイナス（－）の上付き文字は秘密鍵を示す。下付き文字は、鍵の各対の秘密鍵の所有者を示す。

認証機関２３，２５，２７，２９，３１のグループも、ネットワークを介して相互に接続され、署名装置１１，１３，１５，１７，１９とも接続される。各認証機関は、以後で詳細に説明するが、干渉に強いスマートカードやその他の信用装置のように信用コンピュータ装置を用いて活動する人である。認証機関は、ＬＡＮ／ＷＡＮ２１の許す限り分散できるが、認証機関のグループは、署名システムを管理する組織にとって便利なように、ほとんどの場合対応する署名装置の近くに位置している。

図１では、認証機関２ａ（参照数字２５）が例として、また署名装置２が保持している鍵との関係で先に説明したのと同じ記法を用いて説明されている。各認証機関の信用装置にはユニークな名前が付けられる。また、通信の暗号化／復号化のために公開／秘密装置鍵の対２０ａ，２０ｂに、署名の認証や実行のために各公開／秘密装置鍵の対２２ａ，２２ｂについても、同様である。ＲＳＡ公開鍵暗号システムが使われている場合、署名と暗号化の両方に対して同時にこの対が使われる。また、認証機関は、すべての他の認証機関の公開暗号化鍵２４と公開認証鍵２６を受け取る。

また、署名装置は、すべての認証機関の公開暗号化鍵２４と公開認証鍵２６を受け取る。同様に、認証機関の信用装置は、すべての署名装置の公開暗号化鍵２８と公開認証鍵３０を受け取る。

マルチステップ署名のプロセスの説明を簡単にするために、ネットワークでのすべての通信はＲＳＡ鍵転送のような標準公開鍵暗号システム（ＰＲＣ）方式を用いて暗号化されると想定する。また、あるネットワーク法人から別の法人に送

られるコマンドは、ＭＤ５メッセージダイジェストを持ったＲＳＡ署名のように、標準（ＰＲＣ）の方式を用いて送り手により署名されると想定する。以下の図面では、装置暗号化／復号化鍵や装置署名／認証鍵が省かれることがあるが、これは、先に説明したように、すべての装置にあてはまると理解しなければならない。

図２は、安全なデータセンターコンピュータ構成４８の好ましい構造を示している。ここには、図１の各署名装置が存在している。署名装置２９の他に、各データセンター構成４８は、さらに別個のメッセージサーバ４７を含んでいる。署名装置３９は、署名処理専用であり、金庫のような堅固な場所に位置している。署名装置と外部コンピュータネットワークの間は、直接接続されていない。以下で詳細に説明するように、署名装置３９は、マルチステップ署名３６のためのキー部分、自分自身の署名鍵３７、認証機関を識別するテーブル３８、キー部分３６に一致するように選ばれた公開鍵である公開認証鍵４０のための認証を提供される（ここでは、証明書はマルチステップ法を用いてフルKS_{SWA}によって署名される）。

マルチステップ署名プロセスでは、署名装置３９は、メッセージサーバ４７を介して要求を受け取る。メッセージサーバは、介在者が添付している通常のプライバシエンベロープを剥ぎ取ったり（サーバ４７は、署名装置のプライベート復号化鍵を処理しない）、処理速度を越えて提示された場合に行われる入力のキューイングのような通常のの通信プロセスを実行する。メッセージサーバは、署名のために署名装置にメッセージを提供し、署名（または部分署名）結果を受け取り、(a)部分署名結果を要求者に返すか、(b)結果をプロトコルの次の装置に渡す。通常の通信プロトコルを受け取り、そのプロトコルに参加するために、メッセージサーバは、暗号化したメッセージを受け取り、開くことができるように、自分自身のメッセージに署名するための公開／秘密鍵の対３２、３３を所有し、暗号化のための他の対３４、３５を所有する。これにより、安全な署名プロセスのセキュリティを大きく損うことなく、このルーチン負荷から署名装置を解放する。

メッセージサーバ４７は、通常の安全なデータセンタのような、セキュリティ

レベルの低い環境にある、比較的セキュリティレベルが低いコンピュータでも差し支えない。メッセージサーバ４７は、ＬＡＮ／ＷＡＮ ２１に接続し、署名装置３９に文書キューイングや通信サービスを提供する。メッセージサーバ４７は、署名装置との間で送受したメッセージや文書の監査証跡を保守するシステムログ４９を含んでいる。先に示したように、署名装置とその関連メッセージサーバは、通常２つの物理的に別個のコンピュータに分けられる。あまり好ましいことではないが、署名装置３９とメッセージサーバ４７は、安全性の高い環境では同じコンピュータの２つのタスクとして実現することもできる。

メッセージサーバは、署名装置に渡る前にすべての取り引き入力の妥当性を検査する、いわゆるファイアウォールという保護層を提供することもできる。この保護層が提供されない場合、パブリックネットワークにアクセスできるオンラインの署名装置は、サービスの停止を狙ったネットワーク飽和攻撃ばかりでなく、無制限のハッキング攻撃に晒される恐れがある。停止攻撃は日々の証明書発行を中断することができるが、既に署名付き文書に頼っているユーザ（参加ユーザの大部分を占めている）を損うことはできない。しかし、特にハッカーが隠れた瑕疵を識別している場合、ハック攻撃は脅威になりうる。メッセージサーバは、可能な攻撃を識別し、誤ったデータ入力の源を追跡するために高度なアクションを取るという複雑な戦略ばかりでなく、公認の装置（署名装置と認証機関）のリストに対するすべてのメッセージを検査することができる。これにより、署名装置のファームウェアが簡単になり、検査しやすくなるばかりでなく、システムオペレータは、ネットワークセキュリティの現在の状態を基にして自分の検査／回避戦略を変更することができるようになる。

図３は、認証機関のためのワーキングステーションを示している。認証機関として活動するオペレータは、通常ビジネスオフィスに見られるデスクトップコンピュータやターミナル５１のような比較的セキュリティが低いエリアで作業することがある。このようなコンピュータやターミナルは、カードリーダ５３を持っており、各オペレータは安全なスマートカード５５を持っている。各スマートカード５５は、そのスマートカードに固有の、秘密復号化鍵と秘密署名鍵を含んで

いる。オペレータは、カードを用いて署名指示を発行することができる。このような信用装置は、Santa Clara, ＣＡのNational Semiconductor Corp.

社製のiPowerカードのように、FIPS レベル-３装置を用いて実現することができる。なお、このiPowerは、安全な署名や許可の方法や手順が出現すれば、物理装置を交換することなしに、それに合わせてファームウェアレベルで再プログラミングが容易にできる装置である。各認証機関の信用装置は、少なくとも１つの秘密署名鍵を持っていなければならない。通常、秘密署名鍵は、製造者によって装置にインストールされ、対応する公開認証鍵は製造者によって検査される。ここで、検査とは、信用装置に、製造者が、その型番号やその他の信用特徴の証拠の外に、装置のシリアル番号や公開鍵を含んでいる電子メッセージを含め、そのメッセージ（証明書）に製造者が署名するという意味である。

オペレータは、メッセージを読んだり作成したりするのに自分のデスクトップコンピュータを使う。オペレータがメッセージに署名したいとき、デスクトップコンピュータは、メッセージを信用装置に送り、この信用装置は、装置秘密署名鍵を用いて、ディジタル署名を追加する。好ましい実施例においては、この署名は特に特定のユーザのために作成され、検査された２番目の署名鍵の対の署名である。このようにして、システムは、ユーザの識別や同意を取り引きに対して証明するためにユーザの署名を使うと共に、ある取り引きでの装置の信頼性レベルを確認するために装置の署名を使い続けることができる。これにより、ユーザの身元や権限に関する管理事実に応じて、ユーザ鍵を遠隔で作成したり、取り消したりすることができる。また、装置を再利用したり、他の関係ない目的のためにユーザが使うことを望む他の複数のユーザ鍵の対のためのサービスを提供したりできるようになる。

図３は、信用装置が認証機関によって使われる構造を示している。これは、スマートカードという構成で、カードに含まれている１つのマイクロチップからなっている。マイクロチップ装置は、電源と通信のための入出力回路４２と、ファームウェアプログラム実行のためのマイクロコントローラ４２を持っている。メモリ５２は、マイクロチップのハードウェアを駆動するシステムファームウェア

４３（いわば、簡単なオペレーティングシステム）を含んでいる。メモリ５２は、製造者が組み込んだ装置鍵４５、ここで説明するプロトコルの一部として受け取るユーザ鍵４７、そして、ここで説明するネットワークプロトコルを実行するた

めのアプリケーションファームウェア４９を保存するための領域を含んでいる。必要な際の一時的記憶装置として、未使用メモリがワークエリア５４として提供される。また、マクロチップは、暗号化／復号化や署名プロセスの加速数値演算を実行するためのハードウェアを持つ専用数値演算アクセラレータユニットとしての暗号化ユニット４６をオプションで含んでいることもある。さらに、マイクロチップは、製造者によって初期設定され、タイムスタンピング署名に有用なオプションの信用タイムクロック４８を含んでいる。そのために、適切なバッテリ電源が必要である。さらに、マイクロチップには、暗号化／復号化プロセスで使われるオプションの乱数生成器５０を含んでいる。また、スマートカードは、乱数生成で使われる、マイクロチップに内蔵または外付けのダイオードのような図示されないオプションのノイズ源を持っていることもある。

図２に示した署名装置は、認証機関の信用装置と同じ設計のスマートカードであることもある。

ネットワーク上での装置は、以下のような一連の段階を経て初期化される。

１）暗号化鍵の配布

２）署名装置の一時認証

３）キー部分の配布

４）署名装置の再認証

５）認証機関の認証

それぞれを順に説明する。システム初期化の後に、高度な証明書やその他の文書に署名するために使われる通常の方法を説明し、その高度化やバリエーションを取り上げる。

暗号化鍵の配布

各署名装置および認証機関の各スマートカードは、先に述べた特徴に従っての

み動作し、その製造者がプロテクトメモリに保存されている装置署名鍵の対と装置暗号化鍵の対を提供している、改ざんに強い装置であるという意味で、信用装置であると想定している。このような装置の製造者は、最低限、高価な改ざん作業が行わなければ、自分自身のまたはユーザの秘密鍵を漏らさないということを証明しなければならない。また、各装置は、製造者が署名した電子証明書を持っており、その証明書は以下の１）装置シリアル番号、２）装置の公開署名認証鍵、３）装置の公開暗号化鍵、を含んでいる。製造者は、署名認証鍵のためと、暗号化鍵のための２つの証明書をインストールすることができる。署名装置は、公開／秘密暗号法を用いて、自身の通信を暗号化する。または、信用署名装置の代わりに、小さなコンピュータ（ノートブック）が使われる安全な金庫室での、初期化タスクの実行のように、すべての装置に物理的保護を与えることにより、製造者の証明書なしでインストールされることもある。

各信用装置は、ネットワークまたは電子メールシステムを通してメッセージを送受する能力を提供するソフトウェアのような、他の信用装置との相互通信を可能にする特定の基本機能を先ず開始すると想定している。また、先導装置として指定されている１つの署名装置は、システムの初期化を担当するオペレータからシステムの初期状態に関する情報を受け取ることができると想定している。

システム準備の次のステップでは、装置は装置鍵を交換する。鍵配布プロセスは、以下のように進む。

１）先導として指定されている署名装置は、オペレータから、システムの他の署名装置の身元を受け取る。先導装置は、公開暗号化鍵と公開署名認証鍵を他の署名装置に送る。オプションで、先導装置は、ファームウェアをハッシングし、その装置署名鍵を用いてハッシュ値に署名し、署名されたハッシュ値を他の装置に送ることによって、自分のオペレーティングファームウェアを確認するメッセージを送ることもできる。

２）他の署名装置が先導装置の公開暗号化鍵を受け取ると、他の各署名装置は、それぞれの公開署名認証鍵と公開暗号化鍵の証明書を先導装置に送り返す。先導装置がファームウェアのハッシュを送った場合、他の各署名装置は、自分自身

のファームウェアをハッシングし、両方のハッシュを比較する。２つのハッシュは一致していなければならない。一致していない場合、各署名装置は、プロトコルへの参加を停止し、その旨をオペレータに通知する。ハッシュ値のこのような比較により、すべての署名装置は同じファームウェアを用いていることが保証され、先導装置が詐称者でないことがチェックできる。各書名装置は、オプションでそれぞれのファームウェアのハッシュを先導装置に戻す。

３）先導装置は、他の各装置のファームウェアのハッシュを自分のハッシュと比較し、他の装置が詐称者でないことがチェックされる。

ここで、すべての署名装置は、他の装置の公開暗号化鍵と署名認証鍵を受け取っている。以後のすべてのメッセージは、送り手の秘密署名鍵によって署名され、送信者の公開認証鍵を用いて受信者により確認されると、理解される。また、すべての通信は受信者の公開暗号化鍵を用いて暗号化され、受信者の秘密復号化鍵を用いて復号化されると理解される。

これらの追加署名鍵は、以下で説明するマルチステップ署名では使われないが、ネットワーク法人の間での定例通信の暗号化と署名のために、装置の身元の証明として使われる。身元とグループへの所属の証明は、実際のマルチステッププロトコルで使われるマスター鍵の作成と配布の際に非常に重要である。

署名装置の一時証明

図４は、新参の署名装置の一時証明を示している。このプロセスでは、装置の製造者により署名されている、あるいは署名されていない署名装置の公開鍵証明書は、一時管理者（管理者）６１が署名した証明書によって置き換えられる。通常、この管理者は、システムの初期化と管理者のパーソナルスマートカードを使った動作を担当するオペレータである。この一時証明は、マルチステップ署名のために署名鍵を作成する際に使われ、ターゲットグループに属する署名装置の間でのセキュリティレベルを高める。実際には、正しい手順の実行を保証するために一時管理者は複数の人間の立ち会いの下で作業し、一時証明は、完全なマスター鍵作成プロトコルを実行するのに必要な最低限の時間（せいぜい数分または数時間）の間だけ有効であると予想される。

一時証明は、以下のような手順で行われる。

１）管理者６１は、秘密署名鍵６３と対応する公開認証鍵６５を作成する。

２）管理者６１は、各署名装置１１，１３，１５，１７，１９に公開署名認証鍵６５を送る。

３）各署名装置１１，１３，１５，１７，１９は、秘密署名鍵６７，６９，７１，７３，７５と図示されない公開認証鍵を作成し、署名鍵証明要求を管理者６１に送る。署名鍵証明要求は、署名装置の名前、例えば装置シリアル番号及び／又はＳＤ１のような論理名）、装置の新たに作成された公開署名認証鍵、必要に応じてその他の管理情報を含んでいる電子メッセージである。

４）管理者は、管理者の秘密署名鍵を用いて各証明要求に署名する。

５）管理者は、署名した署名鍵証明書６８，７０，７２，７４，７６を各署名装置１１，１３，１５，１７，１９に返す。署名入りの証明書６８，７０，７２，７４，７６は、適切な下付き文字を伴った公開署名鍵(KS^{+})と、その下に添付されている管理者の署名（---ADMIN）の記号として示されている。当然、この証明書は、図示されない装置の身元とタイプに関する情報を含んでいる。

６）署名装置は、自分たちの新しい一時公開署名認証鍵証明書を相互の間で交換する。

この時点で、各署名装置は以下のものを持っている、ａ）管理者の公開認証鍵、ｂ）自分自身の一時秘密署名鍵、３）管理者が署名し、署名装置の一時公開署名認証鍵を持っている一時証明書、４）他の署名装置の一時署名認証鍵証明書。各署名装置は、他の署名装置から受け取った一時証明書における管理者の署名を確かめるために管理者の認証鍵を使うことができる。

各署名装置は、一時管理者が認証した署名鍵を用いて、メッセージを交換することにより、プロトコルのさらに高い段階に進む。以後の説明では、ここから装置再証明までのマルチ署名処理に関わるネットワークでの通信は、一時管理者が証明している署名キーを用いて署名され、各受領者が送信者の署名を認証すると想定する。メッセージに適切な署名がない場合には、メッセージは拒否され、正しいメッセージが提供されない限りプロトコルの継続に失敗する。適切な署名が

ない、あるいは署名されていないメッセージをマルチステップ初期化および署名処理の間に受け取った場合に、なんらかの脅威分析と脅威対策が実行されると想定される。

認証機関の一時証明

図４は、認証機関の一時証明を示している。以下で詳細に説明するが、署名装置は、過半数の認証機関からの許可によってのみ部分署名を添付する。一時管理者の許可の下で活動している署名装置は、過半数の認証機関を要求する。認証機関の一時証明により、指定された人間のエージェントだけが加入時において署名装置を許可できることが保証される。

認証機関の一時証明の手順は、先の署名装置の一時証明の手順と似ており、以下のように進行する。

１）管理者６１は公開署名認証鍵６５を各認証機関２３，２５，２７，２９，３１に送る。

２）各認証機関は管理者６１に対する秘密署名鍵証明要求を作成する。署名鍵証明書要求は少なくとも以下の情報を含んでいる、ａ）認証機関の名前（人間の識別名）、ｂ）認証機関の信用装置の識別コード（例えば、スマートカードのシリアル番号と型番号）、ｃ）認証機関（人間）の署名認証鍵、ｄ）認証機関の信用装置の署名認証鍵（これは、信用装置が既知のタイプであることを保証する）。

３）管理者は管理者の秘密署名鍵を用いて各証明要求３０に署名する。

４）管理者は署名した署名鍵証明書を各認証機関に戻す。

キー部分の配布

図５は、システムワイドオーソリティ（ＳＷＡ９の正式な署名鍵の機能部分（オペレーショナルシェア）の作成と配布を示している。１つの署名装置、ここでは署名装置１（参照数字１１）は、先導装置として指定されている。オペレータは、この先導署名装置に少なくとも以下の情報を提供する。

ａ）鍵を部分に分割するための閾値パラメータ、すなわち作成される部分の総数とＳＷＡ署名を添付するのに必要な最低限の数。

ｂ）公開鍵／秘密鍵の対に割り当てられる鍵識別番号及び／又は論理名、例えば鍵シリアル番号ＫＳ－０１２３４、または論理名ＢＴ０１。

ｃ）各部分に割り当てられるキー部分識別番号及び／又は論理名、例えばＳＷＡ－ＳＨＲ－５６７８９またはＢＴ０１ａ。

ｄ）各装置の特定の署名を最初に許可することが許されている認証機関の装置証明書。

オペレータは、さらに、１つの署名装置において存在しうる断片の総数を制限し、署名装置が複数のマスター鍵を持っている際に使われる数を提供することができる。これについては、以下で詳細に説明する。

次のステップでは、システムを管理するのに使われるシステムワイドオーソリティ（ＳＷＡ）鍵と呼ばれる署名鍵の部分が作成される。公表されたＳＷＡ公開署名鍵と対応する秘密ＳＷＡキー部分が、以下のように作成され配布される。

１）各署名装置１１，１３，１５，１７，１９は、乱数シード情報の暗号化文字列を先導署名装置１１に送る。

２）先導装置１１は、シード情報を結合し、それを用いてパブリックなシステムワイドオーソリティ署名認証鍵（KS_{SWA}^{+}）９１を作成する。この署名認証鍵は、最後に正式署名を認証するのに使われる。

３）先導装置１１は、秘密ＳＷＡ署名鍵の機能部分９３，９５，９７，９９，１０１を作成する。そのために、最初に既知の鍵作成方法を用いて秘密／公開鍵の対を作成し、既知の秘密署名鍵分割方法のいずれかを用いて秘密署名鍵２２を部分に分割する過程が行われることもある。部分の作成には、各部分の最低数ｎ０は、システムワイドオーソリティの署名を完成するのに十分でなければならないという要求が伴う。

４）先導装置１１は、自分のためにＳＷＡ公開認証鍵９１とＳＷＡ秘密署名鍵の１つの部分９３を保存すると共に、ＳＷＡ公開認証鍵９１と１つの秘密署名鍵の部分９５，９７，９９，１０１を他の各署名装置に送る。各ＳＷＡ秘密署名鍵の部分は、以下の追加情報と共に送られる。

ａ）署名鍵部分として鍵を識別するタイプコード（部分の長さも示す）。

ｂ）ＳＷＡ公開認証鍵のユニークな識別コード

ｃ）各ＳＷＡ秘密署名鍵の部分のユニークな識別コード

ｄ）配布される、ＳＷＡ秘密署名鍵部分の総数

ｅ）ＳＷＡ署名を完了するのに必要なＳＷＡ秘密署名鍵部分の最低数

ｆ）他のＳＷＡ秘密署名鍵部分を受け取る署名装置の身元

ｇ）ターゲット署名装置で各ＳＷＡ秘密署名鍵部分の使用を認めることを最初に許されている認証機関の証明書

先導装置１１は、当初の指定の各署名装置の認証済み公開暗号化鍵を用いて各ＳＷＡ秘密署名鍵部分を暗号化する。

５）先導装置１１は、オペレータのために公開ＳＷＡ認証鍵を出力し、以下の情報を消去する。

ａ）作成時のいずれかの時点で秘密ＳＷＡ署名鍵全体が保存されている場合、秘密ＳＷＡ署名鍵全体

ｂ）自分で使うために保存している１つの部分を除き、ＳＷＡ秘密署名鍵のすべての部分

６）各受領署名装置はその装置に対する最初の人間の許可提供者の証明書と共に、不正変更不可能なメモリエリアにそのＳＷＡ秘密署名鍵部分をインストールする。

秘密ＳＷＡ署名鍵は先導署名装置１１だけに、また部分を作成し配布するのに必要な最低限の時間だけ、存在することが望ましい。このようにして、秘密ＳＷＡ署名鍵は、実使用のために存在することがなくなり、攻撃を受ける恐れのある時間は作成時の短時間だけである。

この段階で、各署名装置は、以下のものを安全に受け取っている、ａ）公開ＳＷＡ署名認証鍵のコピー、ｂ）秘密ＳＷＡ署名鍵の部分。

以下で例を示すために、ＳＷＡ署名を添付するのに必要な部分の最低限の数ｎ０は、５つの部分中の２つであると想定している。セキュリティを上げるためにより大きな数（多くの場合少なくとも３つ）を選ぶことができるが、それにより署名プロセスでのステップ数が増加することが理解されなければならない。

署名装置の再証明

初期化プロトコルの前のステップでは、一時管理者６１は、一時管理者６１の権限の下で装置署名認証鍵を証明し、署名装置証明書は管理者の一時署名鍵によって署名された。再証明時には、各署名装置は、他の署名装置の間にある自分の公開鍵がマルチステップ署名を用いてシステムワイドオーソリティキーの下で証明されることを求める新しい証明要求を回覧する。

図６は、署名装置１を再証明するためのステップを示している。他の署名装置は、各装置にこのプロセスを繰り返すことによって自分自身を再証明する。署名装置１のプロセスは、以下のように進む。

１）署名装置１は、未署名の証明書１０３を作成し、その証明書を署名装置２に送る。証明書には、少なくとも以下のものが含まれている、ａ）署名装置の身元（例えば、シリアル番号及び／又は装置論理名）、ｂ）装置の署名鍵の公開署名認証鍵。再証明されなければならない鍵は、元々プロトコルの開始時に装置によって作成され、最初は一時的に管理者によって証明されたのと同じ公開鍵である。この鍵は、この特定のＳＷＡ鍵の部分を扱う署名装置のファミリーに属していることの恒久的な証印になる。装置署名鍵とそれに関連する製造者証明書は、このプロセスにおいて変わらず、装置の起源とその特性の証拠として恒久的に保存される。

２）署名装置２は、そのＳＷＡ署名鍵部分９３を用いて部分ＳＷＡ署名を添付する。部分署名は、以下の２ステップで作成される。最初に、署名装置２は、ハッシングされていない証明書に認証面で関係付けられる切り詰められた文字列を作成するハッシュ関数（例えば、ＭＤ５、ＳＨＡ）を適用する。この文字列は、数値（大きな整数）として操作できる２進数として表される。次に、署名装置２は、ハッシュ文字列をそのＳＷＡ署名鍵部分で累乗して部分署名を作成する。すなわち、署名装置２は、以下の式に従って、部分署名になる数値を作成する。

$$--SD2 = (HASH(CERT))^{[KEY\ SHARE\ 2]}\ modulo\ N$$

本文においても、図面においても、署名ブロックを構成するビットの列は、通常、署名者の識別ラベルの前に長いダッシュを付けることによって示されること

に注意すべきである。作成されたブロックは、通常、署名されるデータのブロックの下部に追加される。それ以外の場合も、文脈から明白である。

３）署名装置２は、部分署名が行われた証明書１０５を署名装置３に送る。

４）署名装置３は、既に適用されている部分署名--SD2 累乗することによってシステムワイドオーソリティ署名を完成する。すなわち、署名装置３は、以下の式に従って、数値を計算する。

$$--SD3 = [--SD2]^{[KEY\ SHARE\ 3]} \text{modulo } N$$

$$= ((HASH)(CERT)\exp KEY\ SHARE\ 2)\exp KEY\ SHARE\ 3)$$

$$= --SWA$$

署名装置によって添付された部分署名を、監査証跡として文書に添付したままにしておくことも許される。この簡単な例では、部分署名は2つしか要求されなかったことに注意すべきである。

５）署名装置３は、署名した証明書を署名装置１に戻す。戻された署名装置１は、証明書のコピーを他の署名装置に配布し、他の署名装置がその署名を認証できるようにする。

この例では、署名装置２、３は、この順序で署名を添付した。数が最少数のｔ０を越えている限り署名装置のいかなる組み合わせでも、またいかなる順序でも署名し、同じ署名を作成することができる。

署名装置のフルシステムによって実行される以後の処理はＳＷＡ署名によって証明されている装置（例えば、以下で説明するように、許可提供者の装置）からの要求に対してのみ実行されることが望ましいので、再証明は重要である。署名装置自身は、他の署名装置に対する要求を行うことができる。この手順により、署名装置自身が、ここで定義するマルチステップ署名プロセスを用いて、システムワイドオーソリティ（ＳＷＡ）全体によって証明される最初の装置になる。

先の再証明プロセスの代替実施例においては、ターゲット装置のグループが、先導装置による初期鍵作成の前に自分の再証明要求（署名なしの証明書）を送付する。先導装置は、断片に分割し、鍵全体を消去する前に、ＳＷＡ秘密署名鍵を作成する時点でこの証明書に署名する。システムの主要な機能は高度に統制され

、しかも効率的内やり方でかかる証明書に署名しなければならないので、こうしたやり方には特別の利点は存在しないように思われる。

認証機関の再証明

図７と図８は、認証機関を証明し、登録するステップを示している。図７は、全体的なシステム構造を示し、図８は、証明要求の処理手順を示している。署名装置は、システムワイドオーソリティの正式署名を認証機関の証明書に添付し、各認証機関の公開署名認証鍵を証明する。登録プロセスにおいては、各署名装置は、署名装置にその部分署名を適用するように指示する力を持っている特定の認証機関の内部保存テーブルを更新する。ルーチンの処理時に、署名装置は、以下で詳細に説明するように、要求が最低数の一時証明またはＳＷＡ証明されている認証機関によって署名されている場合、または最低数の個別署名メッセージを受け取った場合にのみ、その部分署名を添付する。認証機関３ａ（ＡＡ３ａ）を証明し、署名装置３にＡＡ３ａを登録するプロセスは、以下のように進行する。

説明のために、署名装置３と１（図７の参照数字１５、１１）は、ＳＷＡ署名を添付するために選ばれた５つの署名装置の内の２つであると想定している。

１）認証機関３ａは、ＬＡＮ／ＷＡＮ ２１を通じて、署名装置３に再証明要求を送付する（図８の参照数字１２１）。あるいは、許可及び／又は登録を、アクセス制限の設定されている通信チャネルを通した署名装置への直接接続に、例えばスタンドアロンコンピュータへの直接接続に制限することができる。証明要求には、少なくとも以下の情報が含まれている；ａ）認証機関の名前（人間の識別名）、ｂ）認証機関の信用装置の識別コード（例えば、スマートカードのシリアル番号や型番号）、ｃ）認証機関（人間）の署名認証鍵。これは装置が既知のタイプに属することの保証となる。すべてのまたは実質上すべての処理は広く分散した位置から実行され、システムオペレータは目視検査によっては何も認証できないので、このような保証は特に重要である。

２）署名装置３は、パーシャルＳＷＡ署名（－ＳＤ３）を証明書１２１に添付し、部分署名証明書１２３を他の署名装置に送る。

３）署名装置１は、部分証明書をＳＤＩに送れるようにする。

４）署名装置１は、ＳＷＡ署名鍵の部分９３を用いて署名プロセスを完了する。

５）署名装置１は、署名が完成した証明書１２５を署名装置３に戻す。

６）署名装置３は、署名された証明書１１１のコピーを保存し、認証機関１１３のログにＡＡ３ａと入力し、署名された証明書１２５を認証機関３ａに戻す。

署名装置３に登録されなければならないすべての認証機関１０１に対してこのプロセスが繰り返され、各認証機関１０１には署名付きの証明書を残し、署名装置３にはすべての証明書のログ１１３を残す。他の署名装置１１，１３，１７，１９のすべての認証機関に対して、このプロセスが繰り返される。

マルチステップ署名

この段階で、署名装置は、ＳＷＡ秘密署名鍵の部分によって初期化されている。署名装置は、自分自身を再証明しており、認証機関はその各署名装置で再証明、登録されている。ここで、システムは、システム管理と正式証明機能の両方のためのルーチンサービスに入る準備ができている。以下の説明では、通常システム管理に使われるシステムワイドオーソリティキーについて、マルチステップ署名を説明する。以下で説明するように、追加のマスター鍵も、同じ装置ファミリー

内でのマルチステップ署名のために、システムワイドオーソリティキーの場合と同じように作成され使用される。但し、このマスター鍵によって署名されるメッセージの内容が管理関係でない場合は例外である。

図９と図１０は、システムワイドオーソリティキーを使ったマルチステップ署名を示している。図９は、様々な認証機関と署名装置を通る文書（ＤＯＣ）の流れを示しており、図１０は文書における署名の進展を示している。この例は、認証機関１ａと１ｂによって署名装置１は部分署名を添付できるようになり、認証機関２ａと２ｂによって署名装置２はＳＷＡ署名を完了できるようになると想定している。単純化のために、どれでも差し支えないが、２つの認証機関が各署名装置を活性化するために必要であると想定する。以下のような順序で行われる。

１）認証機関１ａは、ＷＡＮ／ＬＡＮを介して署名要求を受け取る。要求は、

ヘッダ１３３と署名される文書１３５を含んでいるメッセージ１３１である。ヘッダは、署名要求としてメッセージを指定するコマンドコードを持っている。

２）認証機関１ａ（図９の参照数字１３２）は、ヘッダを抜き出し、いくつかのチェックを実行して文書に署名すべきかどうか判断する。オペレータの判断を含むことができ、また文書の基本目的によって異なることもある特定の手順チェックは、マルチステップ署名プロセスそのものと密接な関係はない。文書に署名すべきであると判断すると、認証機関１ａは、ＳＷＡ署名の下で再証明されている認証機関の秘密署名鍵を用いて文書に署名する。図１０に示すように、認証機関１ａの署名（--AA1a）は、文書のハッシングとＡＡ１ａの秘密署名鍵を使ったハッシュの累乗によって決められる。ＡＡ１ａは、新しいヘッダを添付し、署名した文書１３７を認証機関１ｂ（認証機関１ａと同じ署名装置のための別の認証機関）に送る。

３）認証機関１ｂ（図９の参照数字１３８）は、ヘッダを抜取り、いくつかの手順チェック（マルチステップ署名とは密接な関係はない）を実行して文書に署名すべきかどうか判断する。証明書に署名すべき判断すると、認証機関１ｂも文書に署名する。図１０に示すように、ＡＡ１ｂの署名（--AA1b）は、以下のものによって決められる、１）文書とＡＡ１ｂの署名の連結結合のハッシング、

２）ＡＡ１ｂの署名鍵を使ったハッシュの累乗。ＡＡ１ａの署名は、監査証跡として文書に残される。次に、ＡＡ１ｂは、新しいヘッダを添付し、２度署名された文書１３９を署名装置１に送る（図９の参照数字１１１）。

４）署名装置１は、２度署名された文書１３９を受け取り、ヘッダーを抜き取って、文書がその登録済み認証機関の署名を必要な数だけ、この例では２を持っているかどうかチェックする。持っている場合、署名装置１は認証機関の署名を抜き取って、部分ＳＷＡ署名を添付する。図１０に示すように、部分ＳＷＡ署名（--SD1）は、認証機関の署名のない基本文書をハッシングし、署名装置１のＳＷＡ署名鍵部分９３を用いてハッシュを累乗する。次に、署名装置１は新しいヘッダを添付し、部分署名文書１４１を別の署名装置の認証機関、ここでは、署名装置２の認証機関２ａに送る。

５）認証機関２ａ（図９の参照数字１４３）は、ヘッダを抜取り、いくつかの手順チェック（マルチステップ署名とは密接な関係はない）を実行して、文書に署名すべきかどうか判断する。証明書に署名すべきと判断すると、認証機関２ａは文書に署名する。図１０に示すように、ＡＡ２ａの署名（--AA2a）は、以下のものによって決められる。１）証明書と部分ＳＷＡ署名（--SD1）の連結組み合わせのハッシング、ｂ）ＡＡ２ａの再証明済み署名鍵を使ったハッシュの累乗。ＳＤ１の部分ＳＷＡ署名は、文書に残される。次に、ＡＡ２ａは、新しいヘッダを添付し、署名入りの文書１４５を認証機関２ｂに送る（図９の参照数字１４７）。

６）認証機関２ｂ（図９の参照数字１４７）は、ヘッダを抜取り、いくつかの手順チェック（マルチステップ署名とは密接な関係はない）を実行して、文書に署名すべきかどうか決める。文書に署名すべきであると判断すると、認証機関２ｂは文書に署名する。図１０に示すように、ＡＡ２ｂの署名（--AA2b）は、以下のものによって決められる、１）証明書、部分ＳＷＡ署名、ＡＡ１ａの署名の連結組み合わせのハッシング、ｂ）ＡＡ２ｂの再証明済み署名鍵を使ったハッシュの累乗。部分ＳＷＡ署名とＡＡ１ａの署名は文書に残される。次に、ＡＡ１ｂは、新しいヘッダを添付し、署名入りの文書１４９を署名装置２に送る（図９の参照数字１３）。

７）署名装置２は署名入り文書１４９を受け取り、ヘッダを抜取り、証明書が登録済み認証機関の署名を必要な数だけ（この例では２）持っているかどうか確認する。持っている場合、署名装置２はその認証機関の署名を抜取り、部分ＳＷＡ署名を修正して、ＳＷＡ署名を完成する。図１０に示すように、完成したＳＷＡ署名（--SWA）は、署名装置２のＳＷＡ署名鍵部分９５を用いて、署名装置１によって添付された部分署名（--SD1）を累乗して決められる。次に、署名装置２は新しいヘッダを添付し、部分署名された文書１５１をＡＡ１ａ（元の認証機関）に送る。

先に説明した例において、システムワイドオーソリティ署名を添付するには２つの署名装置が必要であり、各署名装置は2つの認証機関からの許可を必要とし

た。システムにおいて署名を完成するのに必要な署名装置の総数は、キー部分が作成されるときに調整でき、各署名装置の認証機関の閾値数は、セキュリティのために人間のレビューのレベルに依存して、各署名装置で変わりうる。

先に説明したように、マルチステップ署名プロセスを設定した後に、システムワイドオーソリティキーの存在によって許可されるように、過半数の他の署名装置の同意によって条件付けられている主要な管理業務を実行することができる。これらの管理業務のいくつかについて、以下で説明する。

この業務や決定を効率化するために、それぞれの改ざん不可能な署名装置内のファームウェアを、以下の場合に、署名入りのコマンドに対してのみ応答するようにプログラミングする。

１．適切な過半数の認証機関による部分署名要求の場合

２．システムワイドオーソリティ自身によるシステム管理変更の場合

すなわち、好ましい実施例では、署名装置の許可提供者または関連の要求のリストには、過半数の許可提供者または過半数の署名装置の同意なしには、変更することはできない。暗号化バックアップを実行する許可のように、小さな変更のためにシステム全体の同意を得ることは、不必要に煩雑であるように思えるかもしれない。しかし、通常のビジネス活動の規模と比較した場合、このような管理変更は一般に頻繁に行わなければならないものではなく、システムのセキュリティのためには、そのような同意をいずれの場合でも得なければならないと思われる。例では、ユーザを（再）証明し（再）登録するには、人間による４つの署名だけが必要であることに注意。

パラレル署名

図１１は、マルチステップ署名システムのパラレル実施時における文書の流れを示している。この図では、システムには総数３の署名装置１６９ａ，１６９ｂ，１６９ｃがあり、システムワイドオーソリティ（ＳＷＡ）署名を完成するにはこれら３つの署名装置が必要であると想定している。パラレル署名は、これとは異なる数の署名装置に適合しうると理解されなければならない。

パラレル法では、文書統合器１６１（コーディネータ）は、署名すべき文書１

６３を受け取る。しかし、統合器はいずれかの署名装置の認証機関である必要はないが、統合器は通常、別個の法人として図示される。

文書統合器１６１は、署名すべき文書１６３の３つのコピー１６５ａ，１６５ｂ，１６５ｃ（または、文書のハッシュの３つのコピー）を作成する。各コピーは、最初の認証機関１６７ａ，１６７ｂ，１６７ｃに送られ、次に２番目の認証機関１７１ａ，１７１ｂ，１７１ｃに送られ、次に３つの署名装置１６９ａ，１６９ｂ，１６９ｃのいずれかに送られた後、最後に統合器１６１に戻される。以下で詳細に説明するように、文書統合器は、３つの署名装置の署名を結合し、署名入り文書１７３を作成するために元の文書１６３に添付されるシステムワイドオーソリティ署名（--SWA）を作成する。

図１２は、いずれかのコピーの処理および３つの部分署名のシステムワイドオーソリティ署名への組み込みを示している。各コピーは基本的に同じ処理をされると理解しなければならない。しかし、それぞれの認証機関と署名装置はその個別署名鍵に応じて署名または部分署名を添付するという例外がある。

この例では、各署名装置１６９ａがその署名を添付できるようにするには、２つの認証機関が必要である。統合器１６１は、自分の署名（--AA1a）を添付し、２度署名された署名入りコピー１７５ａを２番目の認証機関１７１ａに送る最初の認証機関１６７に対するルーティング情報ヘッダ（図示されない）と共に、署名する文書の最初のコピー１６５ａを送る。２番目の認証機関１７１ａは、２番目の許可署名を添付し、２度署名された文書１７９ａを署名装置に送

る。署名装置１６９ａは、２つの許可署名を認証し、部分署名（--SD1）をコピーに添付して、署名入りコピー１８１ａを統合器１６１に戻す。

図示されない他の２つの署名装置は、署名される文書のコピーに部分署名を添付し、署名入りコピー１８１ｂ，１８１ｃを統合器に戻す。これら３つのコピーは、パラレルに処理することができる。

統合器が署名すべき文書のコピー３つ１８１ａ，１８１ｂ，１８１ｃをすべて受け取った後、統合器は、３つの部分署名（--SD1，--SD2，--SD3）を掛け合わせる。３つの部分署名の積が、システムワイドオーソリティ署名（--SWA）にな

る。

認証機関の署名装置とスマートカードは、信用装置である。このパラレルマルチステップ署名法のセキュリティは、統合器のワークステーションの物理的セキュリティには依存していない。統合器は、認証機関に許可を与えるために、いかなる秘密鍵も処理する必要はない。しかし、通常、プライバシや識別のためにルーティング暗号化鍵および署名鍵を持っている。

統合器の機能を認証機関の間に配分することもできる。最初の認証機関は、署名すべき最初の文書を受け取り、部分署名を受け取り結合する別の認証機関を指定することもできる。あるいは、いずれかの署名装置のサーバのような認証機関でない別の法人でも指定できる。組織の通常、の運営では統合器に署名すべき文書を受け取ってもらい、署名入り文書の最後の受領者への配送を担当してもらうのが望ましいと思われる。

認証機関の追加／削除

各署名装置は、認証機関の関連グループを持っている。人が組織を出入りするので、システムは、認証機関の信用装置の公開鍵を追加および削除することによって、許可提供者を動的に追加または削除するための決まりを持っている。認証機関の追加または削除は、認証機関の公開鍵の追加や削除を行うコマンドの署名装置への送付によって行われる。コマンドは、追加／削除コマンドのコード、追加情報（以下で説明する）、そして許可署名を持っている電子メッセージの形を取る。

許可署名は、同じ署名装置の他の認証機関から来ることもあり、追加／削除の

プロセスをローカルに１つの署名装置によって完了することもできる。また、追加／削除手順が、システムワイドオーソリティキーの署名を要求することもある。その場合、変更を承認し許可するために関係した過半数の署名装置において過半数の認証機関が必要になる。あるいは、認証機関の能力が異なり、強力な認証機関はシステムワイドオーソリティキーの下で追加または削除できるが、能力の低い許可提供者はローカル過半数の権限の下でローカルに追加または削除できる。、認証機関の追加または削除には、システムワイドオーソリティキーの署名が

必要とされるようにするのが望ましい。

図１３は、認証機関を削除するためのコマンド２０１を示している。コマンド２０３での追加情報には、以下のものが含まれる、ａ）認証機関の名前２０５、ｂ）認証機関のタイトル２０７、ｃ）認証機関が削除される署名装置のＩＤ番号２０９、ｄ）削除される認証機関と関連している信用装置の識別コード２１１。適切に署名されたコマンドを受け取った後、署名装置は、認証機関の公開認証鍵を認証機関の内部リストから削除する。

図１４は、認証機関を追加するコマンド２１３を示している。追加情報には、以下のものが含まれる、ａ）認証機関の名前２１７、ｂ）認証機関のタイトル２１９、ｃ）認証機関が許可される署名装置のＩＤ番号２２１、ｄ）認証機関に認められている権限を示す管理クラス２２５、ｅ）新しい認証機関の権限の終了日２２３、ｆ）認証機関が署名装置に適用するよう指示するマスター鍵の識別コード２２７、ｈ）信用装置の公開署名認証鍵を持っている証明書２３１。新しい認証機関の公開鍵は、ＳＷＡ署名鍵の権限の下で証明され２３３、コマンドに証明書が含まれるのが一般に望ましい。認証機関と結びついている信用装置の製造者が署名した装置証明書２３１も、認証機関の秘密署名鍵が承認済みのミニマムセキュリティプロパティを持っているスマートカードやその他の信用装置に封じ込められるという保証を含んでいる。装置のミニマムセキュリティプロパティには、生物測定情報を用いてスマートカードを人間のユーザの身体的特徴と結び付けるという事実が含まれているのが望ましい。例えば、ユーザが添付の指紋リーダを起動しない場合、カードはユーザ署名を作成しないとすることができる。この場合、一致する指紋データは、カード内部に保存されており、カードを使用するた

めに使われる。適切に署名された要求を受け取った後、すなわち、ＳＷＡマルチステップ署名が完了した後、署名装置は新しい認証機関の情報を認証機関の内部リストに追加する。

カードの製造者や型名の追加／削除

先に説明したように、認証機関は、事前定義セキュリティプロパティを持つよ

うに製造されているスマートカードのような信用装置を通して動作する。認証機関を追加するための条件として、認証機関の信用装置は承認済み型名でなければならない。システムの始動時に、システムで使うことが認められる信用装置の型番号が入力された。新しい型番号が利用可能になり、セキュリティ対策が強化され、次第に古い型番号が受け付けられないようになる。すべての署名装置は、適格な型番号の内部テーブルを保守する。

新しい製造者を追加するために、すべての署名装置の間に電子要求を回覧し、新しい製造者を追加することができる。図１５は、要求のサンプルを示している。要求は、システムワイドオーソリティキーによって署名されたメッセージ２４１にまとめられた、製造者の名前２４５、型名または型番号コード２４７、公開署名認証鍵２４９と共にコマンド２４３を含んでいる。

署名装置のテーブルから製造者の公開認証鍵を取り除くために、ＳＷＡ鍵が署名した電子メッセージを回覧することによって、古い製造者を削除することができる。図１６は、コマンド２５３と製造者の名前２５５を含んでいる要求のサンプル２５１を示している。過半数の装置が署名した、これらの追加／削除要求は、すべての装置に送られ、各装置がその要求をK^{+}_{SWA}を用いて認証し、それに基づいて活動する。

承認済みの製造者の新しい型名は、ＳＷＡ鍵が署名した電子要求を送付することによって追加できる。図１７は、要求のサンプル２６１を示している。要求は、コマンド２６３、製造者の名前２６５、型番号２６７、特定の型番号がセキュリティ基準を満たしていることを示している製造者署名入りの証明書２６９（例えば、この型番号はFIPSレベル３要求を満たしているという証明書）を含んでいる。

古い型番号は、署名装置のテーブルから型番号を取り除くための、ＳＷＡ鍵署名付き電子要求を送付することによって削除することができる。図１８は、コマンド２７３、製造者の名前２７５、型番号２７７を含む要求のサンプル２７１を示している。

署名装置の追加／削除

次第に、システムに署名装置を追加したり、システムから署名装置を削除しなければならなくなる。各署名装置は、ＳＷＡ鍵の部分、または、以下で詳細に説明するマルチステップ署名のための他のマスター鍵の部分、システム上の他の署名装置のテーブルを含んでいる。各署名装置の身元は、以下によって定義される、１）装置識別番号（例えば、シリアル番号）、２）製造者によってインストールされ、製造者の署名の下で証明される鍵、あるいはＳＷＡ署名が再証明する同じような鍵である装置公開認証鍵、３）暗号化メッセージを装置に送るために使われる装置公開暗号化鍵、４）以後所有するユニークな証明済み公開鍵。

新しい署名装置は、ＳＷＡ署名を受け取るために他の装置の間に署名なしの証明書を回覧してから、署名入り証明書を回覧することによって、システムに追加される。証明書には、先に述べたように、識別情報が含まれる。ＳＷＡ鍵によって証明書が署名された後、証明書は、新しい装置を他の署名装置の内部テーブルに追加する指示と共に、すべての他の署名装置に送られる。図１９は、コマンド２８３と証明書２８２を含んでいる指示のサンプル２８１を示している。証明書は、新しい署名装置ＩＤコード２８５、製造者が署名した署名装置の署名認証鍵証明書２８６、やはり装置製造者が署名している署名装置の暗号化鍵証明書２８９を含んでいる、。署名認証鍵と暗号化鍵が１つの証明書に入っていることもある。新しい署名装置が使うキー部分２９１や新しい装置に預けられる暗号化鍵２９２の部分のような他の情報を他の署名装置の間で回覧しなければならない。署名装置をグループに追加すると、以下のことが可能である、１）新しいマスター鍵を作成し、その部分を受け取るためにプロトコルに参加する、２）署名ＳＤの内容を受け取るバックアップユニットとして動作する、または３）破壊されたあるいはサービスから除かれたリビジョンバックアップ署名装置の復旧内容を受け取る代替ユニットとして動作する。

図２０は、署名装置を取り除くためのメッセージ２９３を示している。メッセージ２９３は、コマンド２９５と装置ＩＤコード２９７を含んでいる。

キー部分の保存

署名装置の窃盗や破壊のリスク（結果）は、マルチステップ署名プロセスの能

力と、どの署名装置も単一では署名を偽造することができず、署名を偽造するのに十分な情報を漏らすことはできないという事実によって低下している。したがって、ＳＷＡキー部分を始めとする署名装置の情報内容は、署名装置ハードウェアのアップグレードやバックアップの際などに他の装置に移すことができる。

キー部分やその他の情報のコピーは、特定の署名装置の情報のすべてまたは一部を２番目の装置にコピーするようにという、ＳＷＡ鍵が署名した要求を送付することによって実行される。図２１ａは、送信側装置にそのキー部分のコピーを要求するサンプルを示している。要求は３０１には、以下のものが含まれるのが望ましい、製造者３０５によって２番目の装置を識別している、ＳＷＡ鍵が署名しているコマンド３０３（この製造者は、公認製造者の署名装置リストに載っていなければならない）、型番号３０７（型番号の承認済みリストに載っていなければならない）、シリアル番号３０９、受信装置の公開暗号化鍵を持っている証明書３１１、コピーされるキー部分のＩＤコード３１３（またはその他の指定情報）、送信装置のＩＤ３１５。署名入り要求が適切な送信装置によって受け取られると、送信装置は受信装置の公開暗号化鍵を用いて、そのキー部分と関連情報を暗号化し、次にadd keyメッセージのような暗号化情報を受信装置に出力する。図２１ｂは、送信装置から受信装置へのサンプルメッセージを示している。要求３１４は以下のものを含んでいるのが望ましい。送信装置が署名した（--SD）コマンド３１６、受信装置ＩＤ３１７、送信装置ＩＤ３１８、暗号化キー部分のＩＤコード３１９、キー部分所有者一のＩＤコード３２０。receive shareコマンドは、受信装置で使われる過半数（または、その他の許可提供関係の詳細）を指定することができるが、受け取った鍵は受信装置のデフォルト過半数に従って使われるのが望ましい。一般的な動作手順として、すべてのシステムオペレータや許可提供者には、コピーを保存している装置や記憶媒体の身元と共にコピーが作成されたことが知らされる。

あるいは、情報を、暗号化した形で、バックアップとして使われる物理的に安全な、例えば、金庫室に保管された、そしてオフラインのリモート攻撃を受けることがない記憶装置にコピーすることができる。

過半数要件の変更

ＳＷＡ鍵を添付するのに使われる署名装置の過半数は、キー部分作成時に先導装置によって使われるシステム設計パラメータである。この過半数は、署名鍵全体を回復するためにキー部分を結合し直し、後で元のキー部分と同様に再配布される、新しい過半数要件を持った、より多数の部分に鍵を分割することによって変更することができる。

特定の署名装置が部分署名を添付できるようにするのに必要な認証機関の過半数は、システムを初期化し直さなくても変更可能である。この変更は、各署名装置にＳＷＡ鍵によって署名された要求を送付することによって実行するのが望ましい。あるいは、特定の署名装置の認証機関は、ローカル認証機関だけが署名した要求を送付することによってローカル過半数を変更できる。過半数を変えるのに必要な署名の数は、署名装置がＳＷＡ署名を添付することができるようにするのに必要な数と同じであることも、また異なっていることもある。ＳＷＡキー部分が署名装置内に暗号化した形で保存されており、許可提供者が以下で説明するように復号化キー部分を持っている場合、署名に権限を附与するのに必要な過半数は、ＳＷＡキー部分を復号化するのに必要な部分の数より少なくしてはならない。通常、の銀行業務では、いくつかの許可提供者は複数の署名装置で権限を持っていることがあるが、許可提供者Nは、署名装置毎に２より少なくてはならない。

保存されてるキー部分の暗号化

図２２に示すように、ここでは、１つの署名装置３２１内に保存されている各ＳＷＡキー部分３２３は、暗号化した形３２３で保存されている。復号化鍵（ＫＥＹ）は、部分に分割されており、各認証機関の信用装置３２５，３２７，３２９が復号化鍵の部分を保存している。先に説明したように、署名装置が部分署名を添付するようにという各要求は、過半数の認証機関の署名によって実行されなければならない。この場合、認証機関はさらに復号化鍵３３１，３３３，３３５の部分を署名装置３２１に送る。次に、署名装置は以下のことを行う。

１）復号化鍵３４７を回復するために復号化キー部分３３７を結合する。

２）ＳＷＡ鍵の部分を復号化する３３９

３）平文テキストＳＷＡ部分３４１を用いて、部分署名３４３を文書３４５に添付する。

４）復号化鍵３４７を消去する

５）復号化鍵の部分３３１，３３３，３３５を消去する

６）平文テキストＳＷＡキー部分３４１を消去する３４２

署名を求めて、文書を署名装置に送る際に、認証機関は、その認証機関の復号化キー部分を含んでおり、メッセージに署名する。通常の処理では、復号化キー部分は、ネットワークのすべての通信は受信者、すなわち、文書が認証機関の署名を求めて回覧される際の他の認証機関、または署名のために送付される際の署名装置の公開暗号化鍵を用いて暗号化される。あるいは、各認証機関は、復号化キー部分を保護するために、各メッセージのためのセッションキーを開発することができる。すなわち、鍵を含んでいるメッセージが、ある認証機関から他の認証機関あるいは署名装置に渡されるたびに、新しいセッション暗号化鍵が使われる。その際、メッセージ全体は、セッションキーの下で暗号化される。

このようにして、平文テキストＳＷＡキー部分は、部分署名を添付するために使われている間だけ一時的に存在するにすぎない。さらに、復号化鍵および復号化鍵の部分の完全な組み立ては、一時的にのみ存在する。署名装置が盗まれたとしても、盗んだ者はせいぜいＳＷＡキー部分の暗号化フォームを復元することができるにすぎない。

暗号化キー部分と復号化キーの部分を作成し、配布するプロセスは以下のように進み、そのプロセスは図２３に示されている。

１）先導装置は、基本例において先に説明したように、公開ＳＷＡ認証鍵３５１と秘密ＳＷＡ署名鍵の部分３５３，３５５，３５７を作成する。

２）先導装置は、ＳＷＡ署名鍵の各プライベート部分に対して公開／秘密暗号化鍵の対３５９，３６１を作成する。１つのＳＷＡ部分３５７しか図に示されていないが、他の部分も同様に処理されると理解しなければならない。

３）各秘密暗号化鍵に対して、先導装置は秘密暗号化鍵を、Ｍ分割のＬを用

いて部分３６３ａ，…，３６３ｍに分割する。ここで、Ｍとは部分の総数であり、Ｌとは秘密復号化鍵を再構築するのに必要な部分の最小数である。Ｍは、署名装置の許可提供者の総数と等しい数を選択することができ、Ｌは各ＳＷＡキー部分での署名に権限を附与するのに必要な認証機関の過半数に等しい。

４）先導装置は、関連の公開暗号化鍵３５９の下でＳＷＡ署名鍵の各部分を暗号化し、ＳＷＡ署名鍵の暗号化部分３６５を、各秘密復号化鍵のＭ部分と共に各署名装置に送る。

５）ＳＷＡキー部分の秘密復号化キー部分も、安全のために配布して他の署名装置の間で保管することができる。　これにより、どの秘密復号化鍵も署名装置から回復できるようになるが、どの署名装置といえども、他の装置の復号化鍵を回復するのに十分な情報を持っていない。ある署名装置の一般的な部分が、複数の他のＳＤでの過半数の許可提供者の合意によりリリースされる。

６）先導装置は、秘密復号化鍵、秘密復号化キー部分、（もしまだ存在していれば）秘密ＳＷＡ署名鍵全体をメモリから消去する。

各署名装置は自分の認証機関を登録するときに、署名装置はさらに各認証機関に復号化キー部分を送る。このキー部分は、以下のものによって識別される。１）復号化キー部分の識別番号、２）関連のＳＷＡ部分の識別番号。

例えば、５つのＳＷＡ署名鍵部分が存在し（署名のために必要な３つを含む）、各ＳＷＡキー部分は、別個の公開暗号化鍵の下で暗号化され、各ＳＷＡキー部分は５つの認証機関の内の３つを要求している場合、各復号化鍵は、復号化鍵を回復できる３つを含め５つの部分に分割される。２５の復号化キー部分が存在することになり、それぞれの署名装置は５つを認証機関に自分自身のキーのために分配し、他の４つの装置のために各復号化鍵の１つの部分を持っている。

このようにして、署名装置が部分署名を添付することができるようにするために必要な過半数の認証機関は、署名装置が各署名活動で一時的にＳＷＡキー部分を復号化できるようにするのに十分な数の復号化キー部分を持つことになる。

１つまたは複数の認証機関が自分の鍵を喪失した場合、例えば、信用装置スマートカードを喪失した場合、同じ署名装置に新しいスマートカードが登録される。復号化キー部分は、署名装置が新たに登録された装置に復号化鍵の部分を転送

す

るようにという、ＳＷＡ署名鍵が署名した電子メッセージを送付することによって、他の署名装置から回復でき、新しく登録されたすマートカードにインストールし直すことができる。あるいは、ＳＷＡの同意があれば、受け取り権限を持っている者の信用装置の公開暗号化鍵の下で暗号化するようにして、ある装置がすべての復号化鍵を受け取り、その署名部分を復号化し、新しい暗号化キーペアを作成し、公開鍵の下で署名部分を再度暗号化し、新しい秘密復号化鍵を新しい部分に分割し、この部分を関連の認証機関の信用装置に再配布するようにすることができる。

また、バックアップ法を使えば、復号化キー部分は、米国特許出願第０８／１８１，８５９号と第０８／２７７，４３８号で説明されているように、独立した信託機関にオフラインで保管することができる。

暗号化ハートビート

さらなる防衛策として、各署名装置は、中断された場合に、署名装置が非活性化される定期的データ入力（ハートビート）を受け取るということもある。ハートビートは、署名装置から離れた位置で作成されるので、誰かが署名装置を盗もうとしても、その者はハードビートの発生源を手に入れるために隔離した部屋または地下室に進入しなければならない。ハートビートの発生源を手に入れることができない場合、署名装置は非活性になっているので、何の役にも立たない。

各署名装置がハートビート発生源に暗号化鍵を提供するという実施例もある。ハートビート発生源は、定期的に暗号化したメッセージを署名装置に送る。署名装置が、ハートビート発生源から一定時間の間に最低数のメッセージを受け取ることができない場合、署名装置はその内部メモリを消去するか、他の回避行動を取る。メッセージは空のメッセージや単純なメッセージでよいが、ＳＤによって与えられた公開イーブンキーを用いて、ハートビート発生源が暗号化しなければならない。あるいは、メッセージは、疑似乱数発生器（ＲＮＧ）がハートビート発生源で作成し、署名装置の同期乱数発生器（ＲＮＧ）が認証した疑似乱数文字列でも差し支えない。

署名装置が一定時間の間に少なくとも１つ（あるいは最低数）の発生源からメッセージを受け取れるように、複数のハートビート発生源を設置することができる。１つのハートビート発生源が機器故障または電源故障によりオフラインになった場合でも、早まって署名装置のメモリが引き起こされることはない。ハードビート通信で使われる鍵は、複数の位置の部分にバックアップできる。

あるいは、次のような実施例も考えられる。各署名装置は、ネットワークの関連（サテライト）装置のグループに照会を送り、少なくとも過半数の関連装置が応答する場合にだけ処理を継続する。過半数を要求することにより、不可避の通信障害や通信修理の際にも処理を継続できる。

複雑にはなるが、サテライト装置を使えば物理的セキュリティが追加され、密閉しガードを固めカメラで監視した所で機器をアップグレードする必要はなく、安全性の低い環境でも使うことができる。

署名装置とそのハードビート発生源またはサテライト装置との間の通信回線は、公衆回線でも差し支えない。署名装置が盗まれたとの報告があれば、システムオペレータはその関連のサテライトユニットを非活性化し、通信回線の盗聴や、盗まれた装置へのハートビートの経路変更を阻止することができる。

例えば、署名装置が米国にあり、その関連サテライト装置がヨーロッパにあるとする。署名装置が盗まれた場合、ヨーロッパのサテライト装置はオペレータによってオフラインにされる。ヨーロッパの認証機関が間違った行動をしても、その影響は非常に小さい。なぜなら、サテライトを撤去しても、短期間新しい署名装置を妨害するにすぎないからである。既に署名済みの署名は依然として有効である。あるいは、公衆回線の代わりに、署名装置とそのサテライトあるいはハートビート発生源の間に、安全な物理回線を設置することもできる。

マスター鍵の追加作成

ＳＷＡ鍵を持った安全なマルチステップ署名システムを確立しておけば、他の目的に使われる複数のマスター鍵を作成することは簡単である。ＳＷＡ署名鍵がシステム管理をコントロールしているので、マスター鍵を用いて、他の合法的法人の代わりに使われる他の証明済みメッセージまたは文書に署名することができ

る。他のマスター鍵の作成や管理は、ＳＷＡ鍵と似ているが、中間の一時証明ステップが存在しない。これは、以下のように行われる。

１）１つの署名装置を先導装置と指定する（ＳＷＡ署名鍵を作成したのと同じ先導装置であってはならない）。

２）マスター鍵の部分を受け取る署名装置の公開鍵証明書リストを入力する。

３）マスター鍵の識別コードとローカル名を入力する。

４）署名装置の間に安全な通信チャネルを確立する。各関連した署名装置の暗号化鍵証明書を使うのが望ましい。

５）オプションで、各署名装置から乱数を取得する。

６）新しいマスター公開／秘密鍵の対を作成する。

７）秘密鍵部分を配布する。オプションで、各部分を暗号化し、復号化キーの部分を配布する。

８）保存されている場合、マスター秘密鍵全体を消去し、先導署名装置が保持していないすべての部分を消去する。

このプロセスは、ＳＷＡ署名鍵としてマスター鍵をインストールするために古いＳＷＡ署名鍵が署名したコマンドを各署名装置に送ることによって、ＳＷＡ署名を交換するのにも使うことができる。一般に、マスター鍵は、ＳＷＡ鍵とは別個の用途を持っており、多数のマスター鍵の部分が、署名装置において共存しうる。ＳＷＡ署名鍵以外の既に作成されたマスター鍵は、マスター鍵の断片を削除するための、ＳＷＡ署名鍵が署名したメッセージを送付することによってシステムから消去することができる。

文書と署名の追跡

システムでの文書のフロー管理を容易にするために、署名される各文書にユニークな識別コードを割り当てるのが望ましい。以下の情報を、メッセージサーバや許可提供者が使うために各文書のヘッダに含めることができる。

１）文書に署名するのに使われる鍵の署名鍵識別コード

２）署名を完成するのに必要な部分署名の総数及び／又は既に使われている部分署名の数

３）署名するのに既に使われている鍵の断片の識別コード

４）既に署名している署名装置の身元（例えば、論理装置名）

署名装置のインターロックリング

既に説明したようにマルチステップ署名システムを使ったルート認証機関は、

通常、他の会社や政府組織にある従属認証機関を認定する。大きなマネーセンターが、州政府の主な認証機関を認証しているとする。そして、州政府は自治体を認証している。これにより、既存の政治的、経済的、社会的組織に適合したやり方で、証明プロセスをフレキシブルに分散している。

しかし、各中位層認証機関は、その署名鍵に対して強力なセキュリティを保持しなければならない。銀行、いくつかの大会社、若干の政府組織を除き、複数の高度に安全なデータ処理施設や保存施設を持っている組織はほとんどない。例えば、中位層認証機関は、データセンターや金庫室での処理のような、少なくとも名目的には安全な物理的施設を持っているかもしれないが、先に説明したマルチ装置方式のための複数のサイトを運営する資金を欠いている。あるいは、中位層認証機関は本当に安全な施設を持たないかもしれない。

しかしながら、会社認証機関のような安全性がより低い中位層認証機関は、先に説明したように自分自身署名リングを設定し、この中位層リングを銀行または安全な政府認証機関のようなマスター認証機関の高度に安全なリングとインターロックすることができる。これは、以下の問題を分けることによって実行できる。（１）鍵の所有者と正式の管理、（２）管理とバックアップの責任、（３）装置の物理的所有。

１つまたは複数の中位層署名装置３７５，３７７，２８９を保守する中位層認証機関３７１を自分の安全な位置に持つことによって、図２４に示すようなインターロックリング構造を作成することができる。追加の中位層署名装置３７９，３８１は、マスター認証機関の安全な場所で保守することができ、マスター（ルート）認証機関リング（ここではインターロックリング）３８３を構成する同じ装置３７９，３８１のいくつかまたはすべてを含むことさえできる。マスターの認証機関は、中位層認証機関３８３の署名装置から独立している、複数の署名装

置８３，３８５，３８７を保守することができる。先に説明した署名装置は、追加マスター鍵を保有するのに追加修正を必要としない。追加マスター鍵は、それぞれ各認証機関３１９ａ、３１９ｂによって別々に所有、管理され、追加されたマスター鍵は別のやり方で分類される。

中位層認証機関は、先導装置である自分自身の署名装置を用いて先に説明した

キー作成および部分配布プロトコルを開始し、自分自身の代理人を認証機関３９１ｂとして任命する。新しい認証機関マスター鍵のいくつかの部分は、自分自身の署名装置３７３，３７５，３７７にあり、残りはマスター認証機関３７９，３８１の署名装置にある。緊急の場合に、マスター認証機関組織の代理人に権限の一部を委任することもできるが、署名を発行権限は、依然として鍵所有者の代理人の元に留まる。

したがって、中位層認証機関は、代理人が所有するスマートカードが作成した署名を元にして認証機関の署名のマルチステップ署名を開始し、この要求を自分の署名装置及び／又はマスター認証機関が所有している装置に宛てて送る。確かに、署名装置は、マスター認証機関と同じ位置にはある必要はないが、安全な位置および通信アクセスを持っている他の認証機関の所にあることができる。

完全賃借サービス

安全な施設をまったく持っていない組織でも、証明書を作成したいことがあり、かつ認証機関になることができる。組織は、様々な銀行または他の認証機関によって既に設定されている安全な位置にある署名装置の使用を賃借することができる。組織は、認証機関のためにスマートカードを所有し、通信ネットワークを介して、署名装置宛てに署名要求を送る。したがって、鍵を作成したり、署名を発行したり、その他の管理業務を遂行するプロセスは、所有者との契約に基づいてローカルバンクの物理的コントロール下にある装置内で行われる。

組織の代理人は、自分の新しい署名鍵が作成され、分割され、自分が選んだホスト施設、または、他の銀行や同じ銀行の他の施設のそれぞれに配布されるプロトコルに立ち会うためにローカルで安全なバンキング施設に出かける。その時、必要ならば、適切な管理バックアップ能力を与えることもできる。

次に、組織は、自分自身の安全なローカルセンターまたは地下金庫室を設置することなく、正式の署名や証明書を発行することができる。そして、その際に、既に説明したセキュリティ面でのすべての恩恵を実質的に享受することができる。

署名委任

認証機関が休暇、多忙などのために一時的に利用できなくなったとき、なんらかの形で署名権限を委任することが望ましい。オペレータが自分のスマートカードを－関連のピン番号または鍵を－他人に貸すことは、管理されていないセキュリティリスクが発生するので望ましくない。

元の認証機関（プライマリユーザ）が、代替認証機関（代理人）に特別の委任証明書を発行するという委任機構が考えられる。プライマリユーザが署名した証明書が代理人と代理人の公開署名認証鍵を識別する。委任証明書には、委任証明書と代理人の権限の有効期間が書かれている（Sudia & Ankney, " Commercialization of Digital Signature", １９９３.を参照）。自分のパーソナルスマートカードを使う代理人は、代理人のパーソナル署名鍵を用いて文書に署名し、委任証明書を添える。その結果、文書はプライマリユーザではなく、代理人が署名しているので、文書の受領者は代理人の署名と委任証明書を確認する手順を実行しなければならない。これは、システムのすべてのパブリックユーザがそのような確認能力を持っているかどうか、また満期前に権限をキャンセルしなければならない場合には取り消し情報のソース、またはホットリストへのアクセス権限を持っているかどうかに一部依存する。

実質上、代理人をプライマリユーザ対プライマリユーザのスマートカードに置き換えるという安全なやり方で、代理人がプライマリユーザのスマートカードを使えるようにするのが望ましい。その場合、代理人は、プライマリユーザの署名を添付するためにプライマリユーザのスマートカードを使い、文書の受領者の方は、他の複雑な証明書を認証し、評価するという手間から解放される。

プライマリユーザが署名権限の委任を希望する場合、プライマリユーザは図２５に示すように、代理人に対して代理証明書を発行する。代理証明書は、プライ

マリユーザのＩＤ４１１、代理人のＩＤ４１３、プライマリスマートカードが代理人（おそらくは、代理人の公開認証鍵４１７）を認識する手段、代理証明書４０９（そして、代理人の権限）の有効期間４１５を識別する。プライマリユーザは複数の者を指名し、ある者にはスマートカードを使う権限を与え、他の者のグループには共同してスマートカードを使う権限を与えることができる。このような方法は、既にAddison Fischerにより米国特許第４，８６８，８７７号、同第５，００５，２００号、同第５，２１４，７０２号において述べられている。

図２５に示すように、代理人がプライマリユーザに代わって、文書４０３に署名したい場合、代理人４０１はプライマリユーザのカード４０７に送られる特別のフォーマットで要求４０５を準備し、それに署名する。代理証明書４０９もメッセージに添付されるか、メッセージに含められる。複数の代理人がプライマリユーザのカードの正当性を確認する必要がある場合には、複数の代理人は、先に説明したように複数の認証機関が署名装置に送付される要求に署名するのと同じやり方で要求に順次署名する。署名要求を受け取ると、プライマリユーザのカードは、要求を出しているユーザの署名が、代理証明書で指定されている公開鍵と一致するかどうかチェックし、プライマリユーザの署名４１９を適用し、署名した文書を通常のやり方で署名装置４２１（または、他の宛て先）に送付する。

プライマリユーザのスマートカード４０７を物理的に代理人に渡すこともできる。代理人の権限にタイムリミットがあるのでタイムロックが掛けられる。その結果、代理人は、その期間だけプライマリユーザのスマートカードを使うことができる。先に取り上げたように、プライマリユーザの権限も一定期間に制限されている。この制限により、盗難のリスクが減少し、プライマリユーザと代理人はプライマリユーザのカードを安全性の低いオフィス環境に保存しておくことができるようになる。期限が来ると、スマートカードは、どのような鍵解読攻撃に晒されても解読されることはなくなる。実際に、プライマリユーザまたは代理人が自分のピンを直接カードに記入している場合でさえも、攻撃はまったく無効である。

スマートカードを金庫やロックされた場所に置き、物理的にではなく電子的に

カードリーダにカードを挿入することによって、紛失や物理的攻撃に対する保護策を講じることができる。このようにして、先に説明したすべてのアクションが実行でき、誰もカードを物理的に所有することがなくなる。

例えば、プライマリユーザは、取り引き交渉のため出張に出かけている間、自分の特定の署名権限を秘書に委任したい購買担当副社長でいるとする。代理証明書において、自分のスマートカードは以下の者が署名した署名要求を受け取った場合にのみ副社長の署名を発行すると指定しておく。（ａ）自分の代理証明書で指定した秘書、（ｂ）購入部門で主な署名権限を持っている他の者との共同署名。副社長は、ロックを掛けた金庫の中のカードリーダにカードを差し込み、出張に

出かける。

副社長の署名を得るには、秘書は、署名する文書を準備し、デスクトップコンピュータターミナルを用いて関連のハッシュを計算する。次に、ハッシュに署名し、最終受領者が必要とする、副社長の公開鍵証明書を添付する。そして、他の購入担当者へのメッセージとして送る。受け取った購入担当者は同じハッシュに共同署名し、購入権限を供与している権限証明書と共に自分の公開鍵証明書を添付する。他の購入担当者は、それをローカルエリアネットワークを通して副社長のスマートカードにメッセージの形で送る。副社長のカードは、ＳＷＡのような証明書を作成した認証権限の公開鍵の信用コピーを持っているので、副社長のカードは、署名と証明書がすべて有効であると判断し、副社長の署名を文書に添付する。また、カードは、すべての証明書に最近署名されたＣＲＬを添えること、またはローカル認定のＣＲＬハンドラからの適格証明書を添えるように要求することもできる。

この委任機構は、プライマリユーザのスマートカードをプログラミングし直すことができるという利点を持っている。プライマリユーザのスマートカードは、既知のセキュリティ特徴を持っている信用装置である。継続中のSudiaキー寄託に関する米国特許出願第０８／１８１，８５９号、同第０８／２７２，２０３号で説明されているように、この既知のセキュリティ特徴の１つとして、新しい命

令の安全なダウンロードができなければならないということがある。

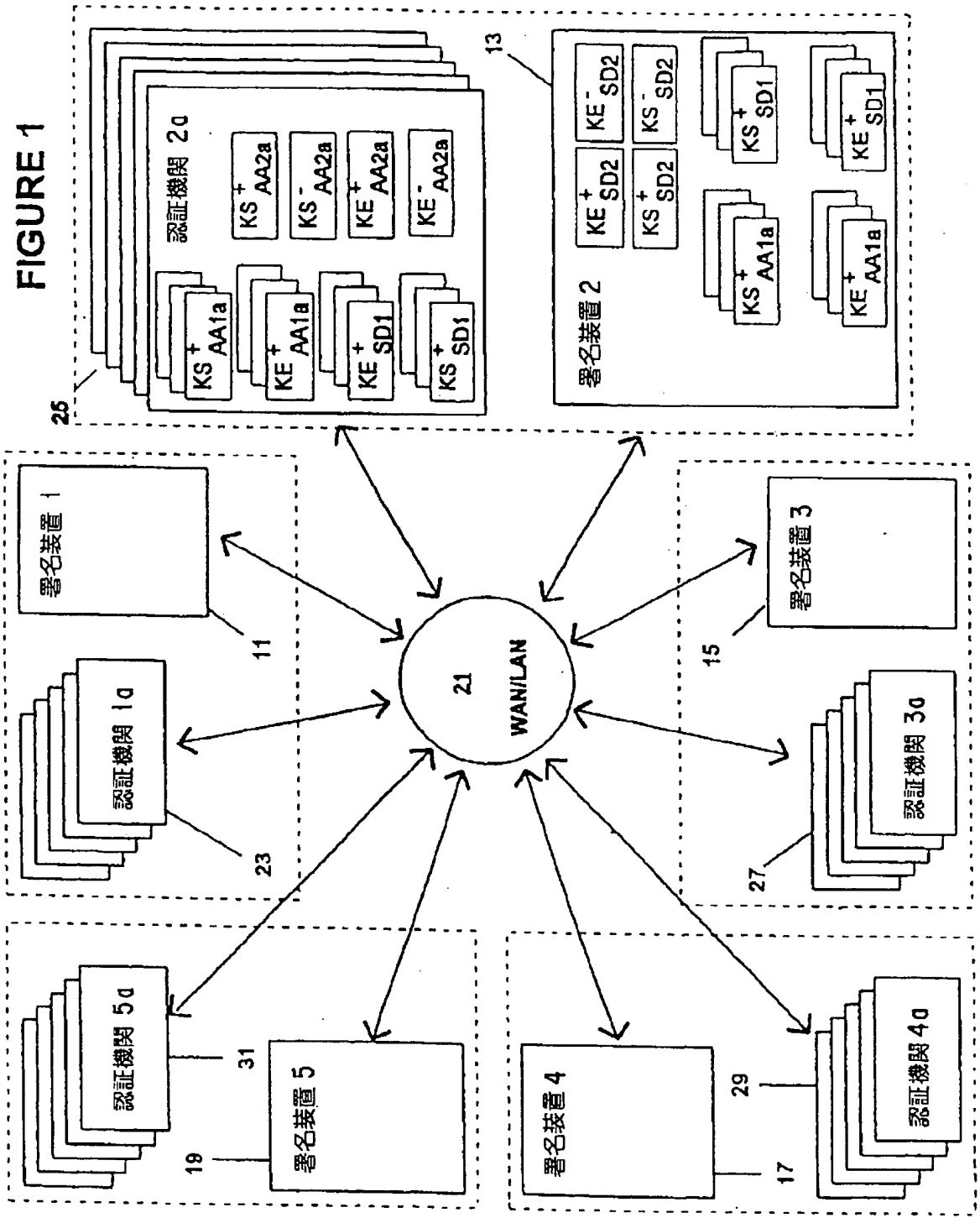
先の寄託機構は、多数の貴重なエンドユーザディジタル署名鍵が、安全な金庫またはデータセンター内に保存されている接近不可能な安全なモジュール（ＴＲＳＭ）内で作成され、使われるように、またそのような署名へのの権限附与が、持ち運ばれる非公式のタイムロックの掛かったスマートカードを与えられる承認済みユーザが署名した署名要求メッセージから来るように、一般化することができる。このＴＲＳＭは、改ざんできないようになっており、データセンターの要員がユーザの秘密鍵にアクセスすることはできないが、非公式な各署名または署名や権限の事前に決まった組み合わせを基にして、それぞれが行動する権限を与えられている多数の各ユーザの鍵を含むように設計される。

一時休暇を取っているユーザからの単純な委任は別にして、次のような委任機構が存在する。このシステムまたは方法では、財務または会社環境の中で主要な役割を果たしているデスクとしての署名を実行するようにという、プログラマチックな署名要求が、カード（または、共通ＴＲＳＭに含まれている鍵）に出される。

前述の実施例を学んだ後に、当業者は、本発明の主旨と範囲内で様々に変更することができる。前述の実施例は、例にすぎず、以下の請求の範囲で定義している本発明の範囲に不当な制限を設けようとするものではない。

【図１】

FIGURE 1


署名装置 1
11
認証機関 1a
23
署名装置 2
13
KE+ SD2
KE- SD2
KS+ SD2
KS- SD2
KS+ AA1a
KE+ AA1a
KS+ SD1
KE+ SD1
認証機関 2a
KS+ AA2a
KS- AA2a
KE+ AA2a
KE- AA2a
KS+ AA1a
KE+ AA1a
KS+ SD1
KE+ SD1
25
21
WAN/LAN
署名装置 3
15
認証機関 3a
27
署名装置 4
29
17
認証機関 4a
署名装置 5
31
19
認証機関 5a

【図２】

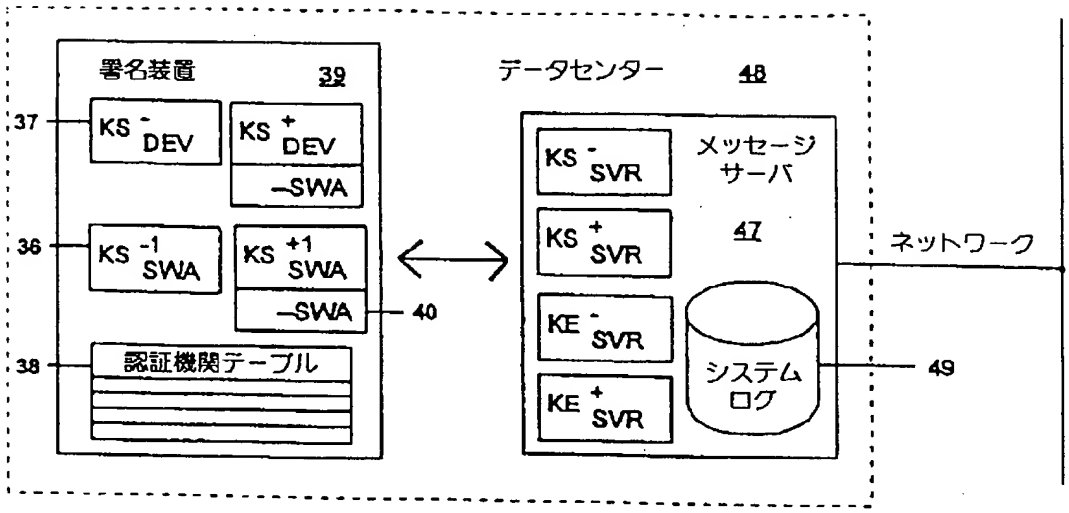


FIGURE 2

【図３】

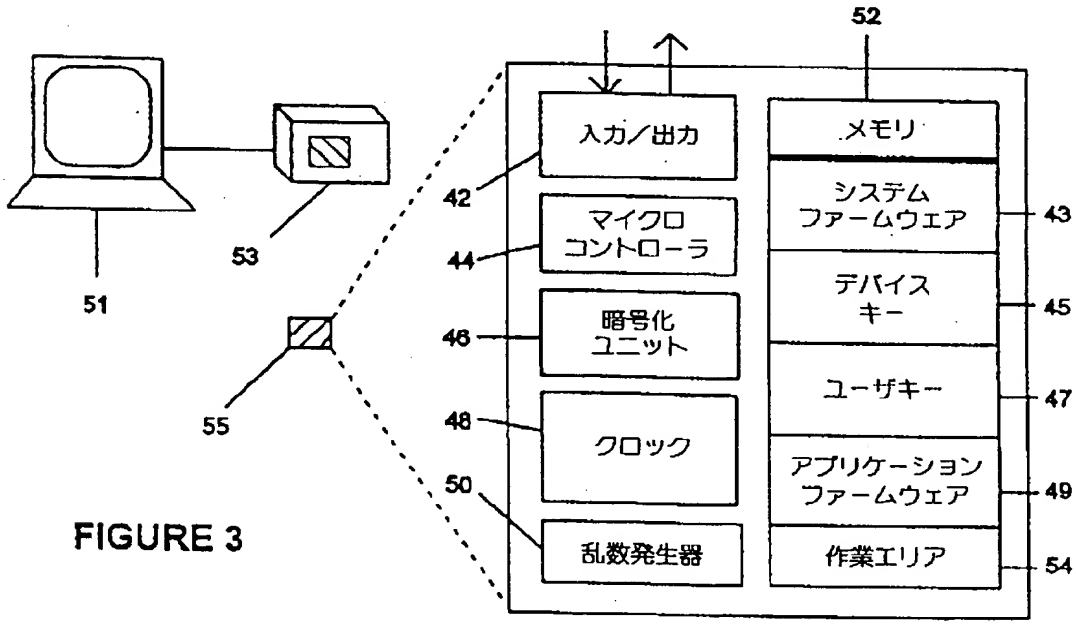


FIGURE 3

【図４】

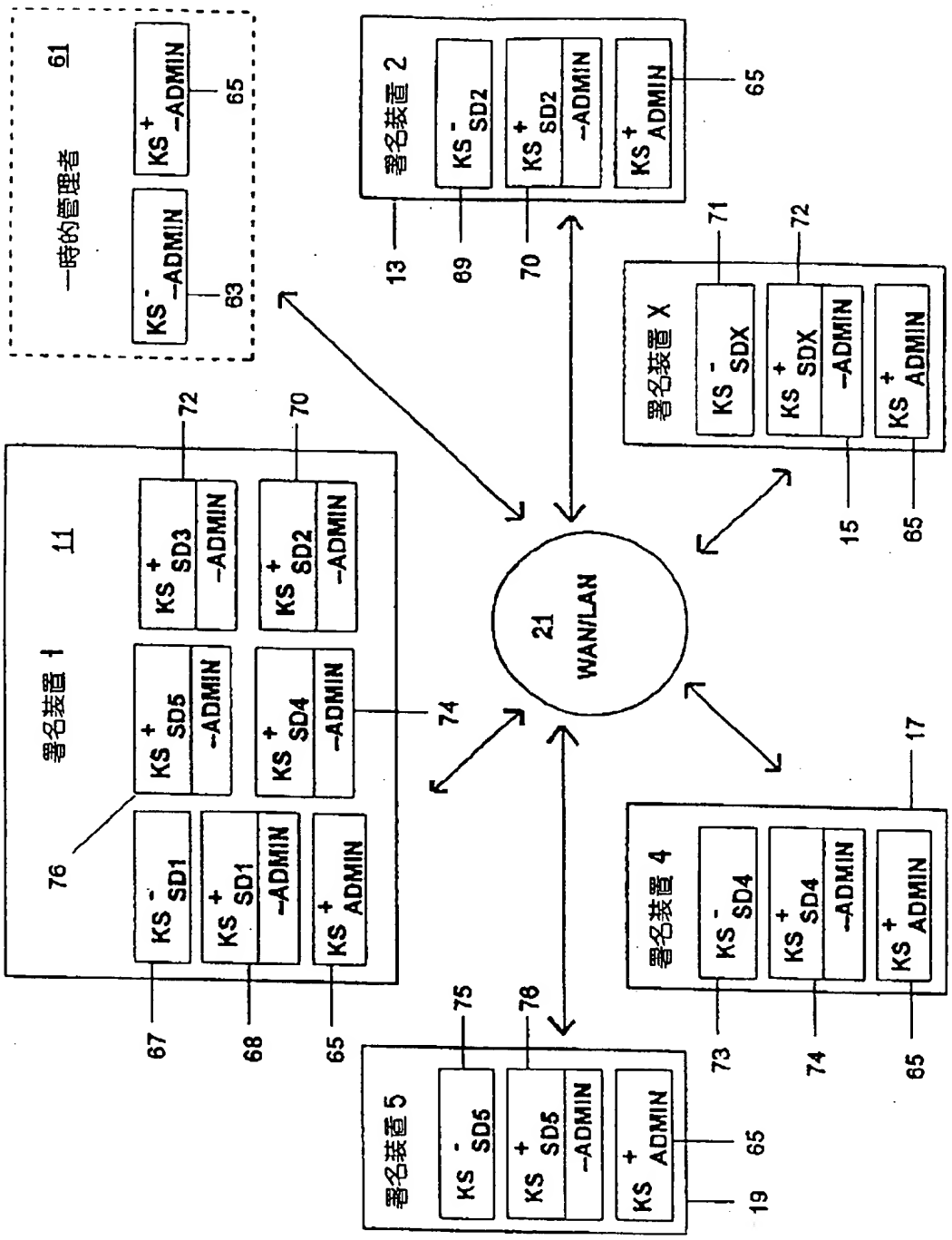

61
一時的管理者
KS+ -ADMIN
65
KS- -ADMIN
63
署名装置 2
KS- SD2
KS+ SD2 -ADMIN
KS+ ADMIN
13
69
70
65
署名装置 X
KS- SDX
KS+ SDX -ADMIN
KS+ ADMIN
71
72
15
65
11
署名装置 1
KS+ SD3 -ADMIN
KS+ SD2 -ADMIN
KS+ SD5 -ADMIN
KS+ SD4 -ADMIN
KS- SD1
KS+ SD1 -ADMIN
KS+ ADMIN
72
70
74
76
67
68
65
21
WAN/LAN
17
署名装置 4
KS- SD4
KS+ SD4 -ADMIN
KS+ ADMIN
73
74
65
75
78
署名装置 5
KS- SD5
KS+ SD5 -ADMIN
KS+ ADMIN
65
19

FIGURE 4

【図５】

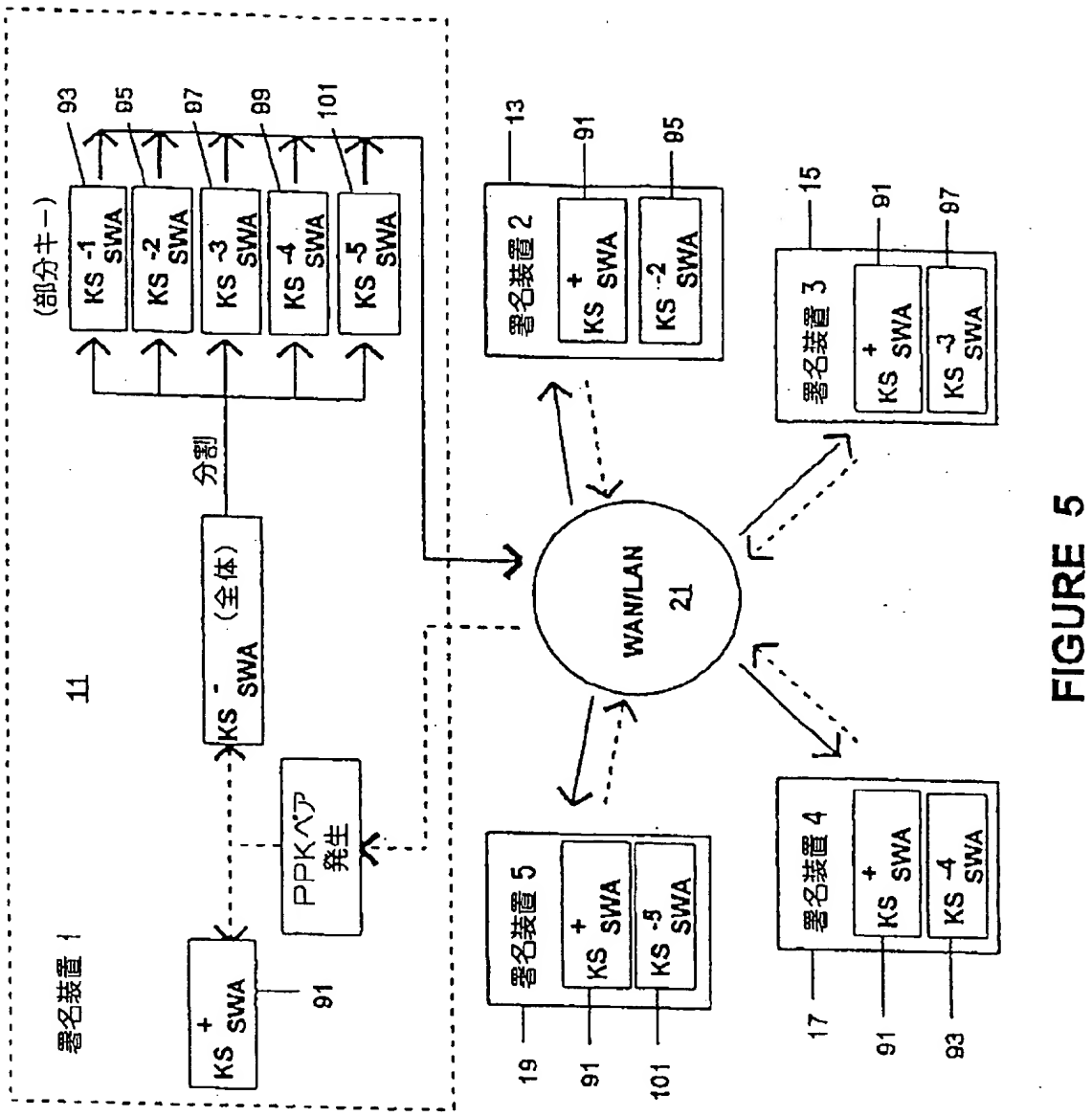

署名装置 1
11
(部分キー)
KS -1 SWA
KS -2 SWA
KS -3 SWA
KS -4 SWA
KS -5 SWA
93
95
97
99
101
分割
KS - SWA (全体)
PPKペア発生
KS + SWA
91
WAN/LAN 21
署名装置 2
KS + SWA
KS -2 SWA
13
91
95
署名装置 3
KS + SWA
KS -3 SWA
15
91
97
署名装置 4
KS + SWA
KS -4 SWA
17
91
93
署名装置 5
KS + SWA
KS -5 SWA
19
91
101

FIGURE 5

【図６】

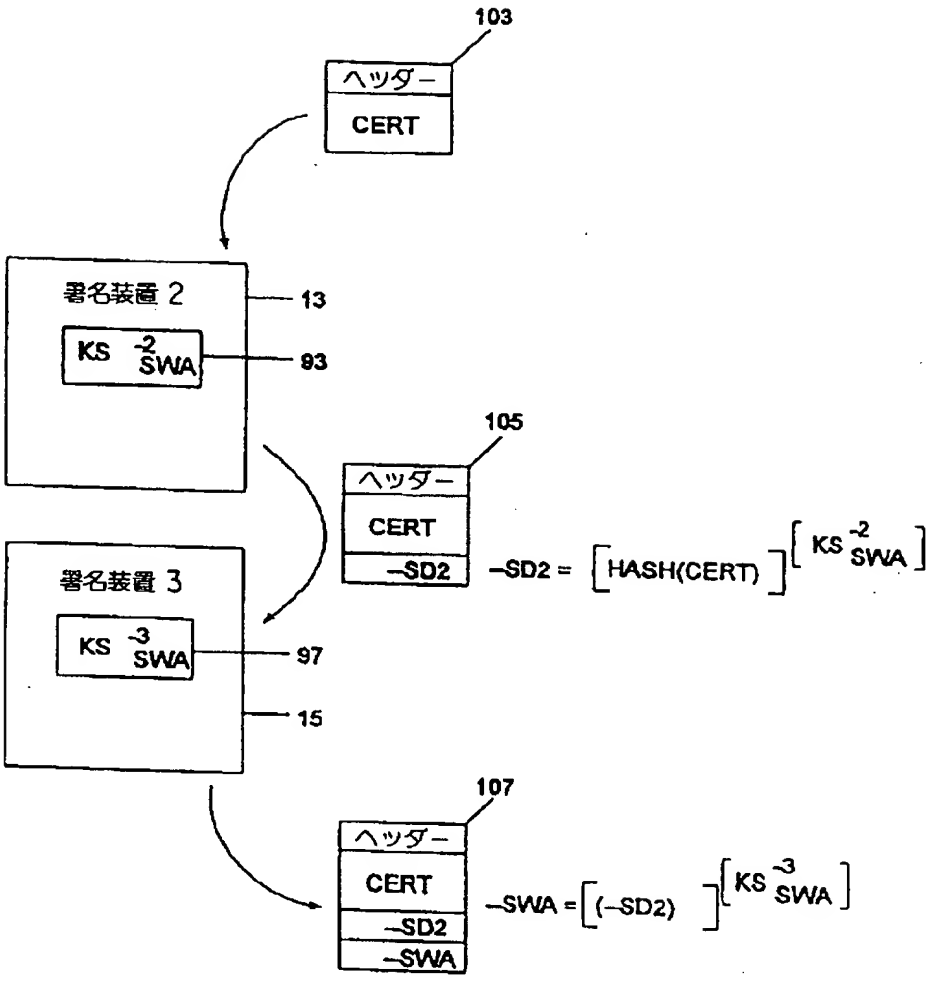

103
ヘッダー
CERT
署名装置 2
13
KS -2 SWA
93
105
ヘッダー
CERT
–SD2
–SD2 = [HASH(CERT)] [KS -2 SWA]
署名装置 3
KS -3 SWA
97
15
107
ヘッダー
CERT
–SD2
–SWA
–SWA = [(–SD2)] [KS -3 SWA]

FIGURE 6

【図７】

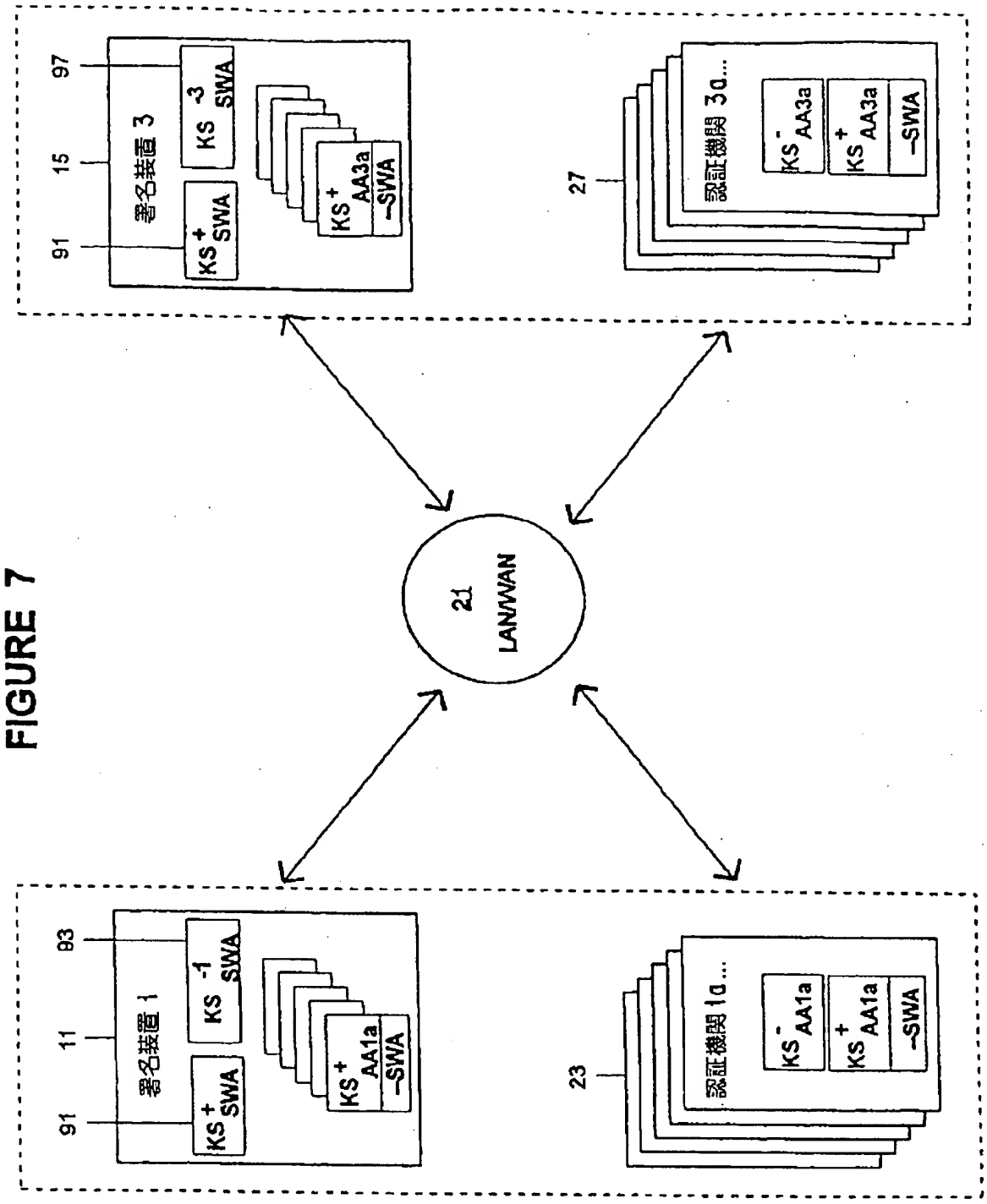

署名装置 3
97
15
91
KS -3 SWA
KS +SWA
KS +AA3a –SWA
27
認証機関 3a...
KS -AA3a
KS +AA3a
–SWA
21
LAN/WAN
署名装置 1
83
11
91
KS -1 SWA
KS +SWA
KS +AA1a –SWA
23
認証機関 1a...
KS -AA1a
KS +AA1a
–SWA

FIGURE 7

【図８】

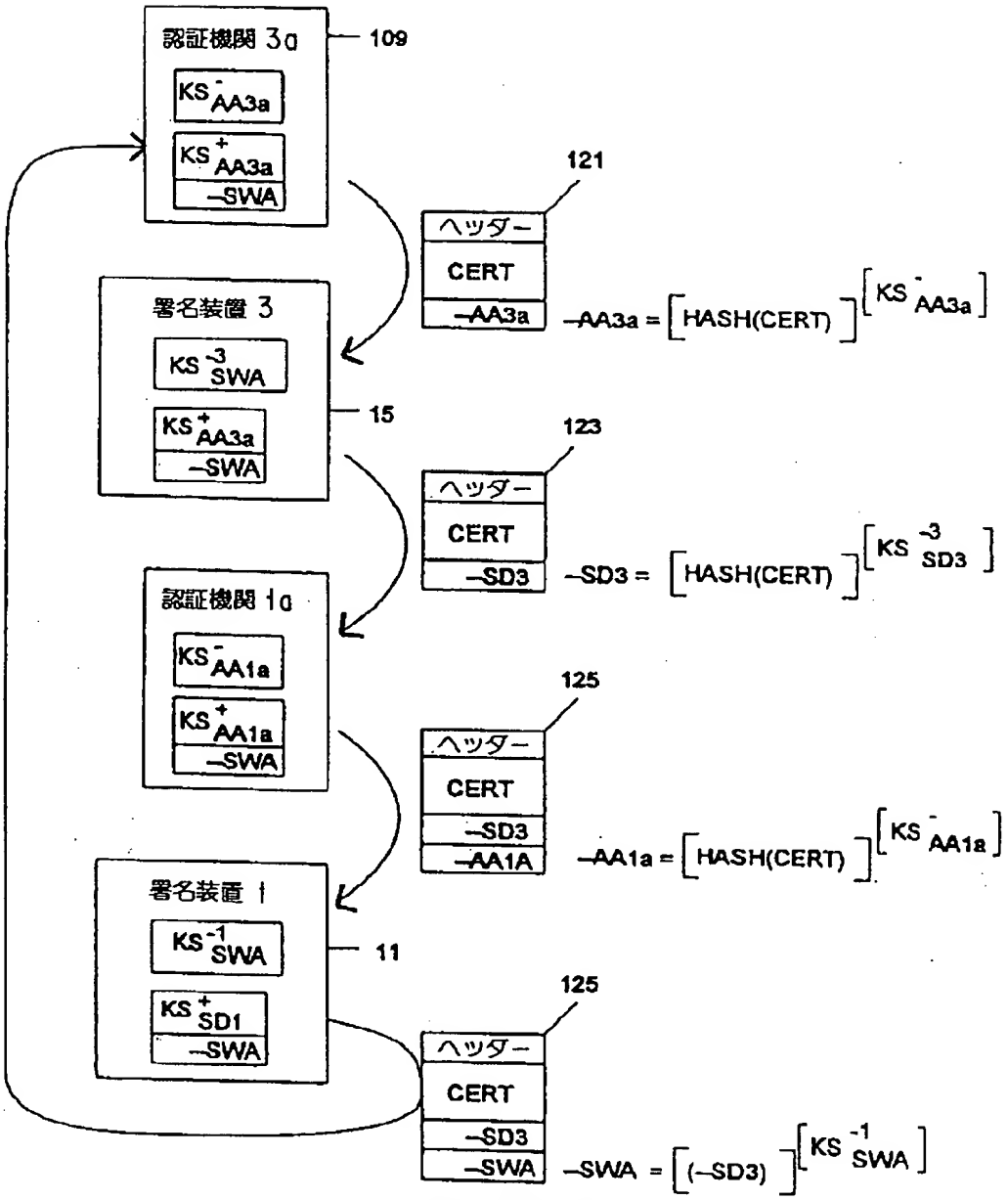

認証機関 3a
109
KS -AA3a
KS +AA3a
–SWA
121
ヘッダー
CERT
–AA3a
–AA3a = [HASH(CERT)] [KS -AA3a]
署名装置 3
KS -3 SWA
KS +AA3a
–SWA
15
123
ヘッダー
CERT
–SD3
–SD3 = [HASH(CERT)] [KS -3 SD3]
認証機関 1a
KS -AA1a
KS +AA1a
–SWA
125
ヘッダー
CERT
–SD3
–AA1A
–AA1a = [HASH(CERT)] [KS -AA1a]
署名装置 1
KS -1 SWA
KS +SD1
–SWA
11
125
ヘッダー
CERT
–SD3
–SWA
–SWA = [(–SD3)] [KS -1 SWA]

FIGURE 8

【図９】

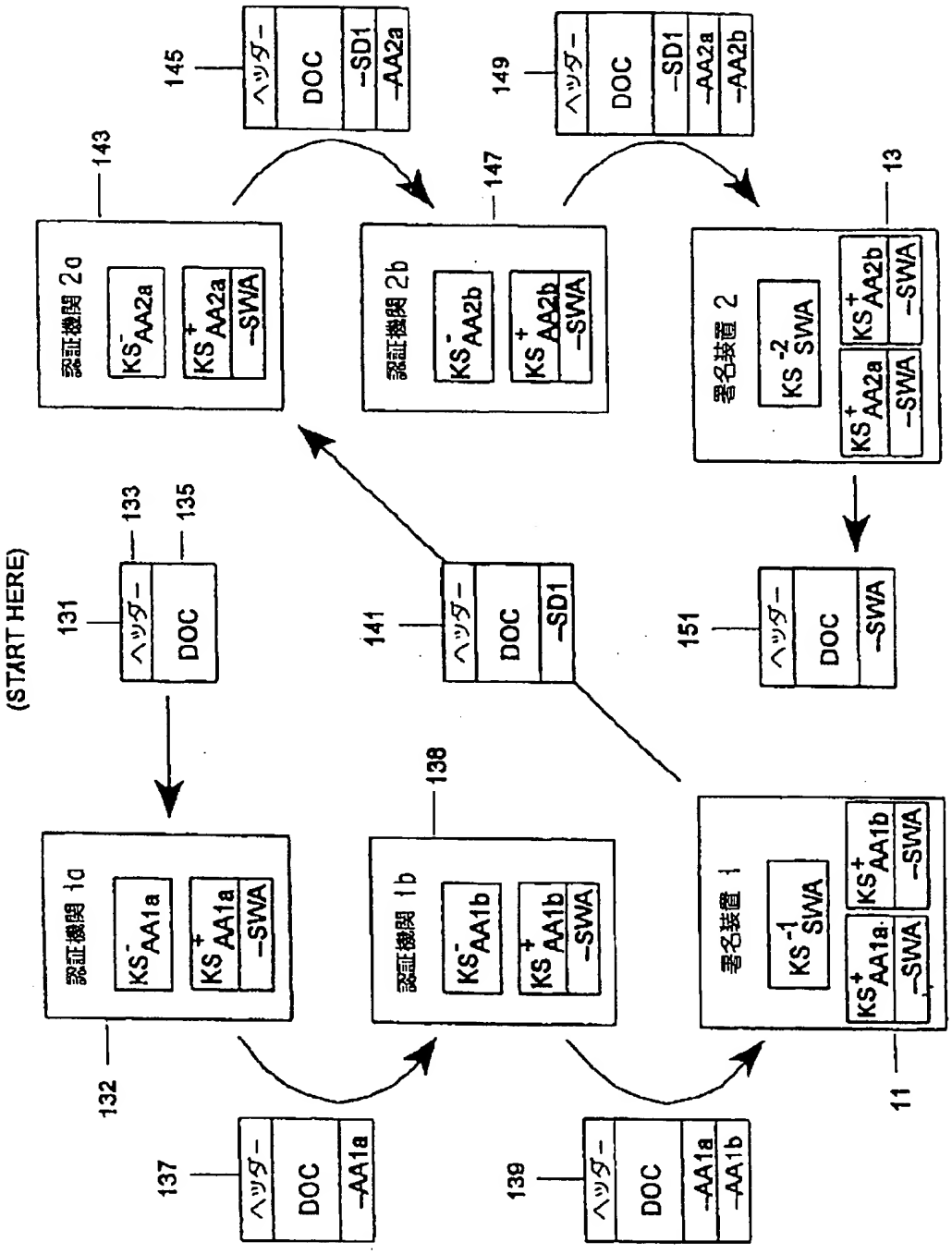

(START HERE)
131
133
135
DOC
ヘッダー
SD1
AA2a
AA2b
AA1a
AA1b
SWA
141
145
147
149
151
143
13
132
137
138
139
11
認証機関 2a
認証機関 2b
署名装置 2
認証機関 1a
認証機関 1b
署名装置 1

FIGURE 9

【図１０】

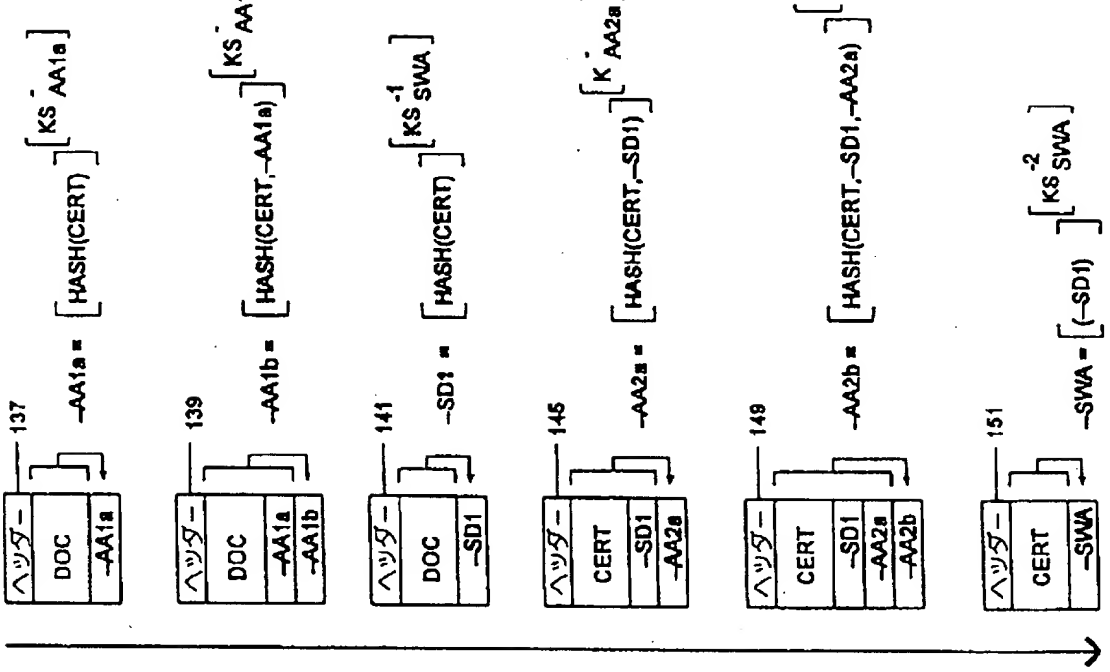


FIGURE 10

【図１１】

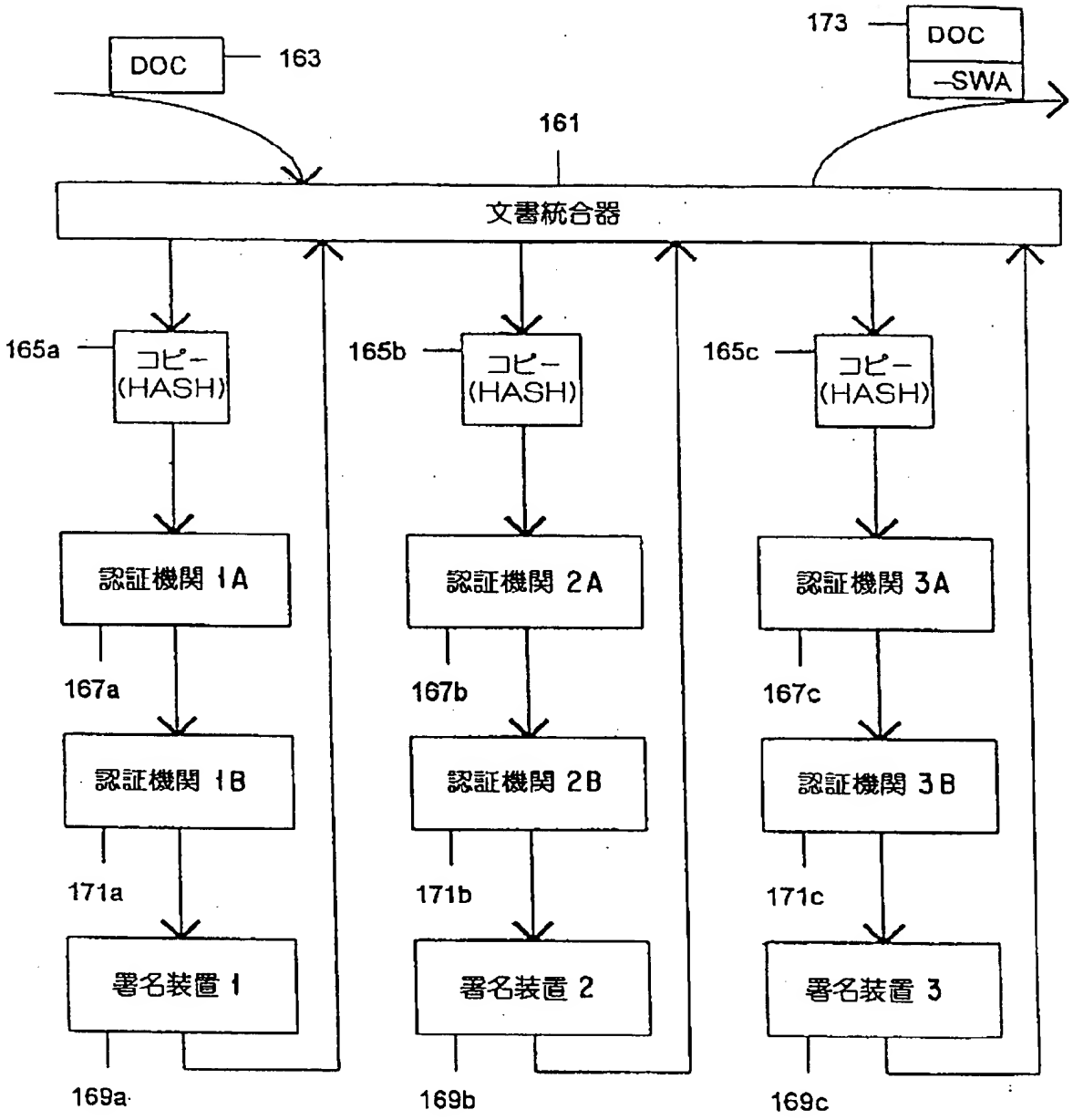


FIGURE 11

【図１２】

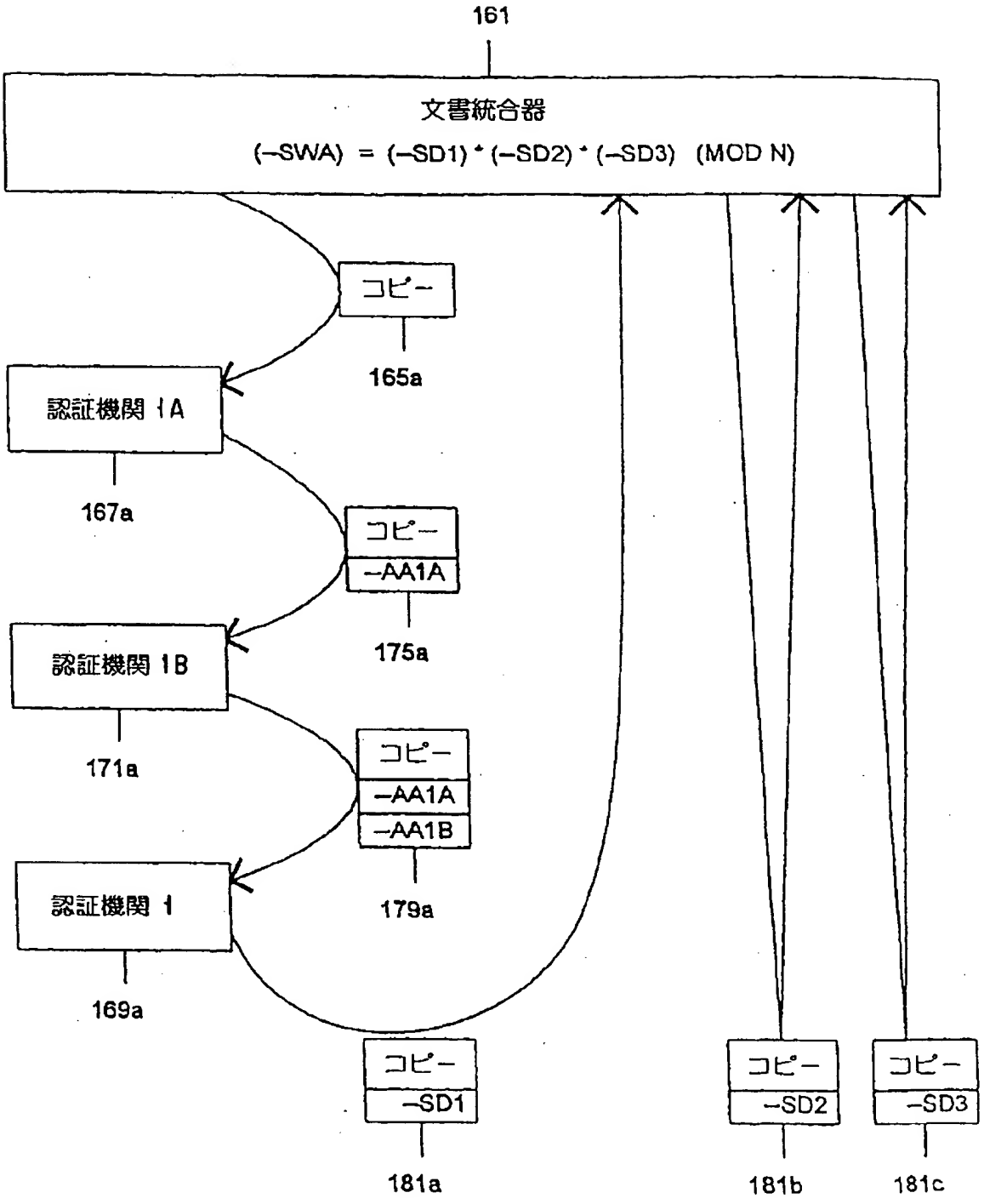


FIGURE 12

【図１３】

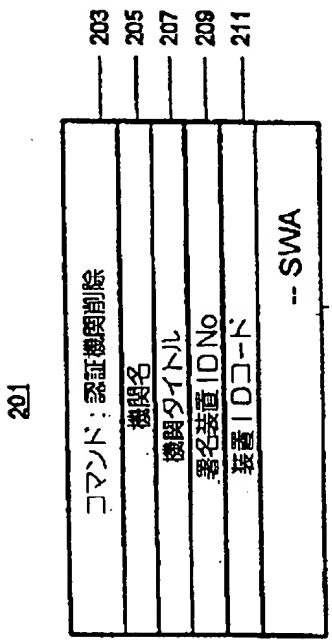


FIGURE 13

【図１４】

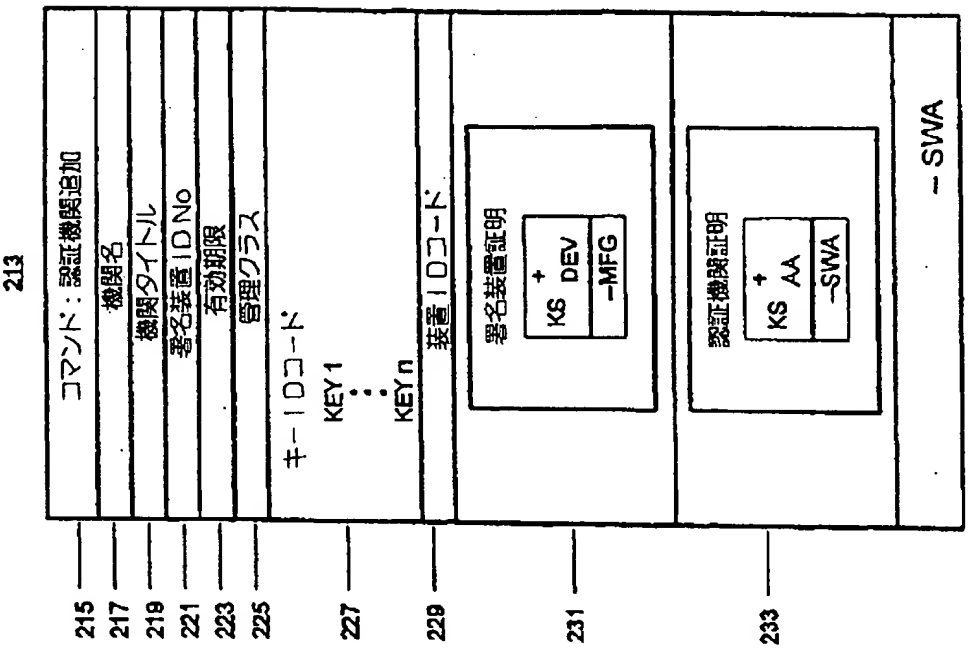


FIGURE 14

【図１５】

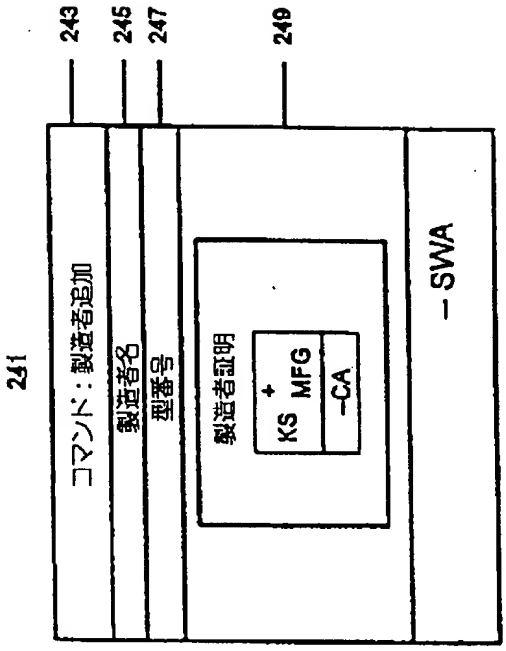


FIGURE 15

【図１６】

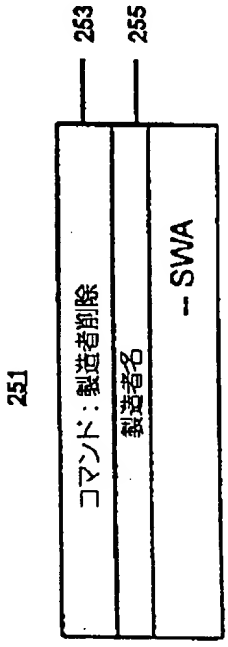


FIGURE 16

【図１７】

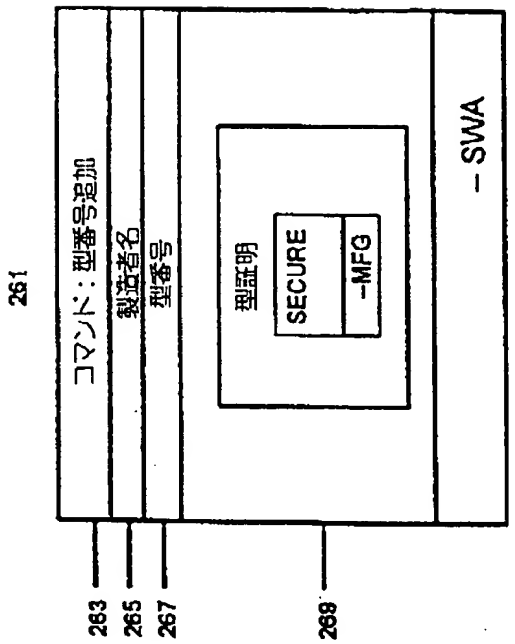


FIGURE 17

【図１８】

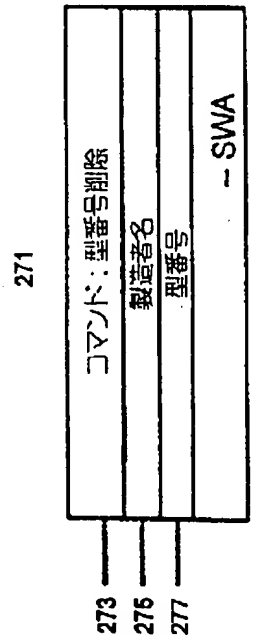


FIGURE 18

【図１９】

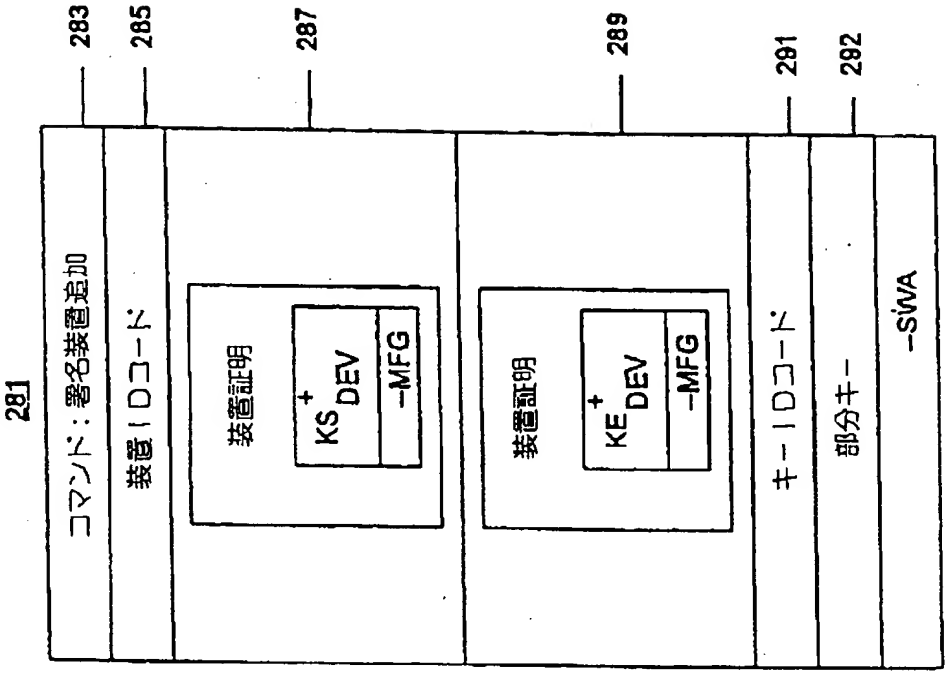


FIGURE 19

【図２０】

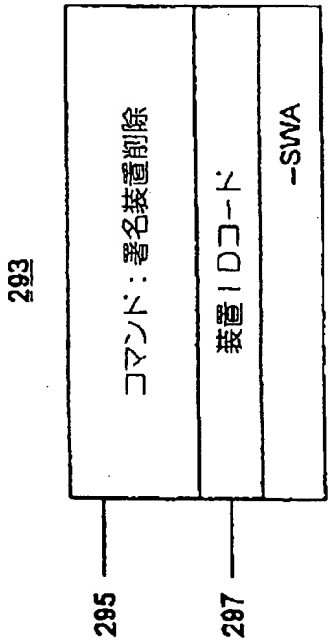


FIGURE 20

【図２１】

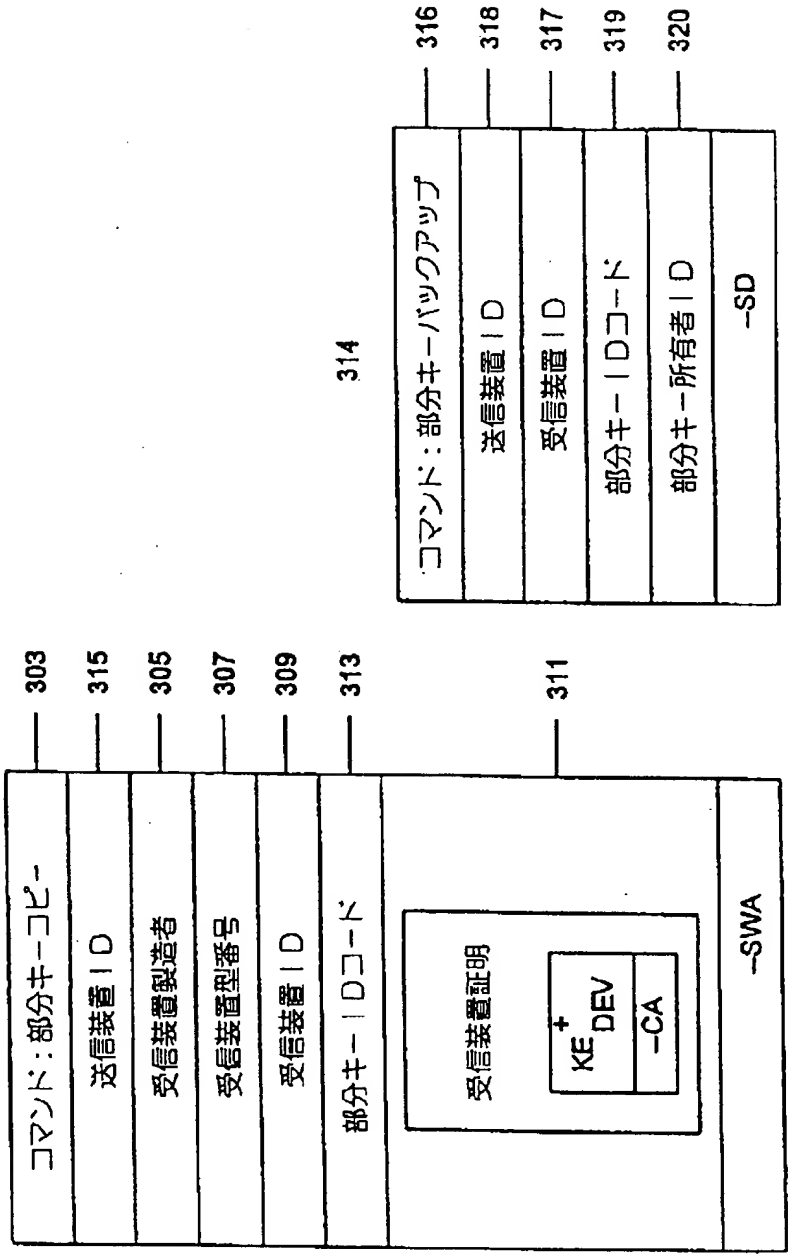


FIGURE 21a

FIGURE 21b

【図２２】

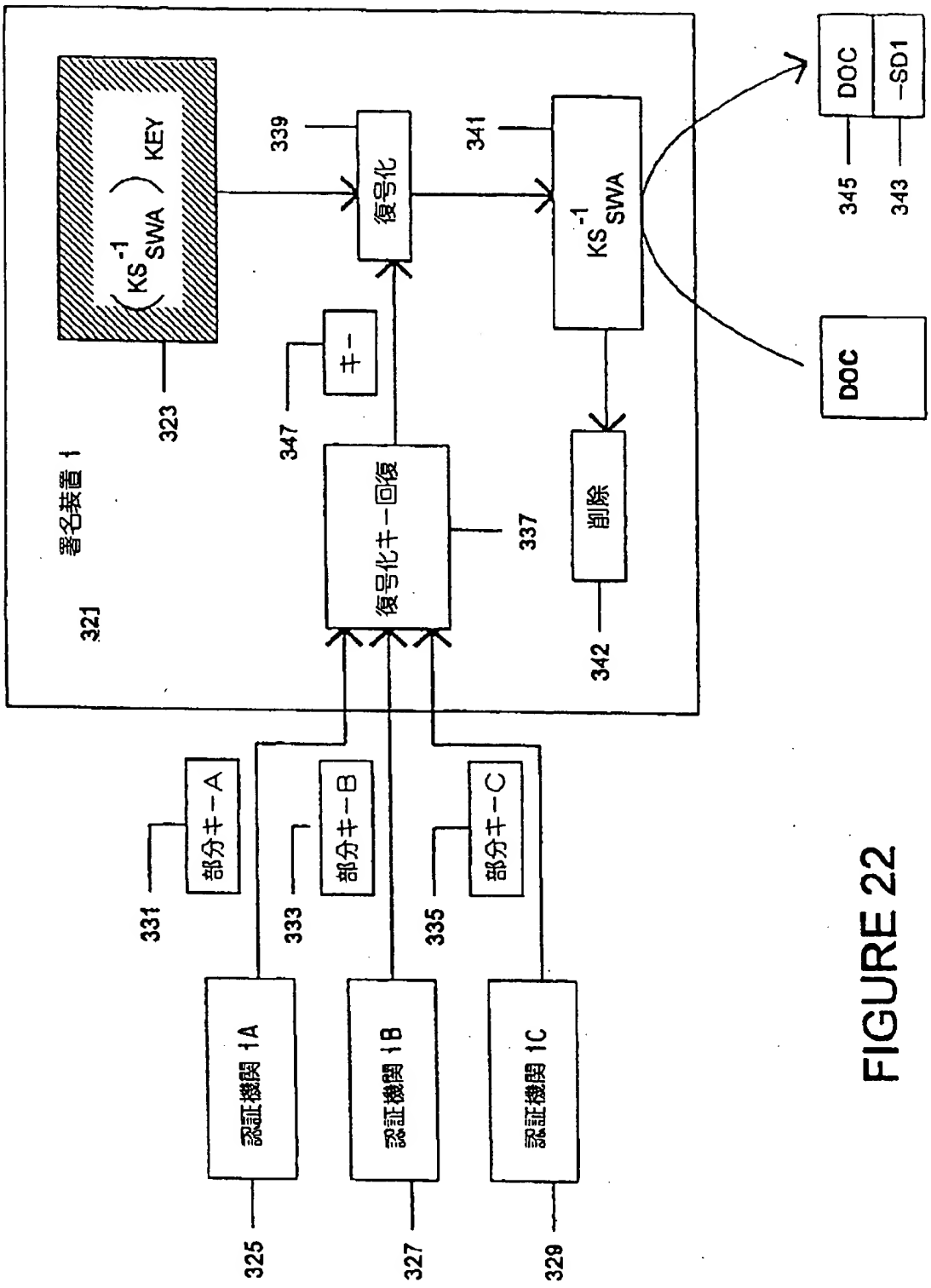
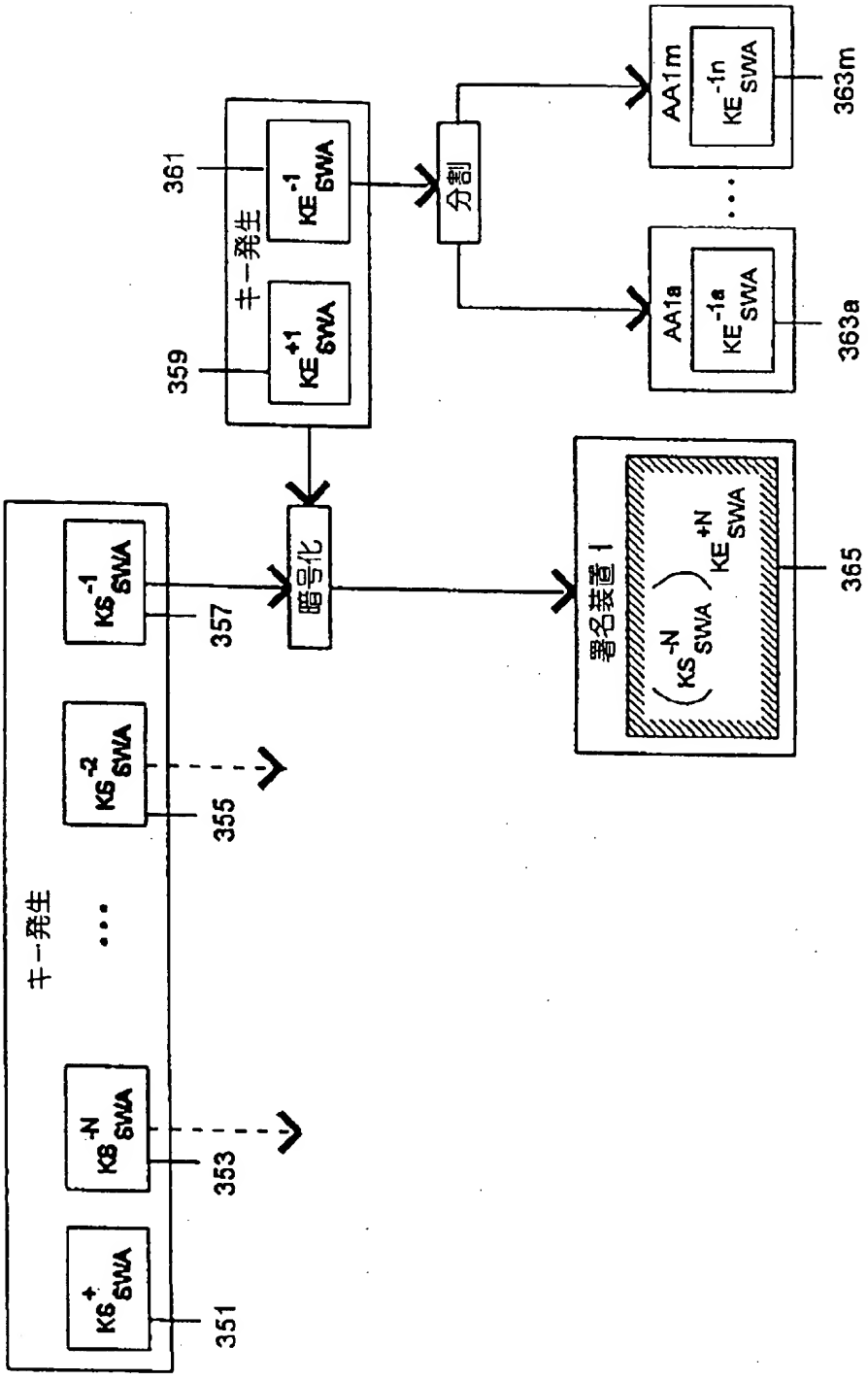


FIGURE 22

【図２３】


キー発生
$K6^{+}_{SWA}$
$K8^{-N}_{SWA}$
KS^{-2}_{SWA}
KS^{-1}_{SWA}
351
353
355
357
暗号化
キー発生
KE^{+1}_{SWA}
KE^{-1}_{SWA}
359
361
分割
KE^{-1a}_{SWA}
AA1a
363a
KE^{-1n}_{SWA}
AA1m
363m
署名装置 I
$(KS^{-N}_{SWA})\ KE^{+N}_{SWA}$
365

【図２４】

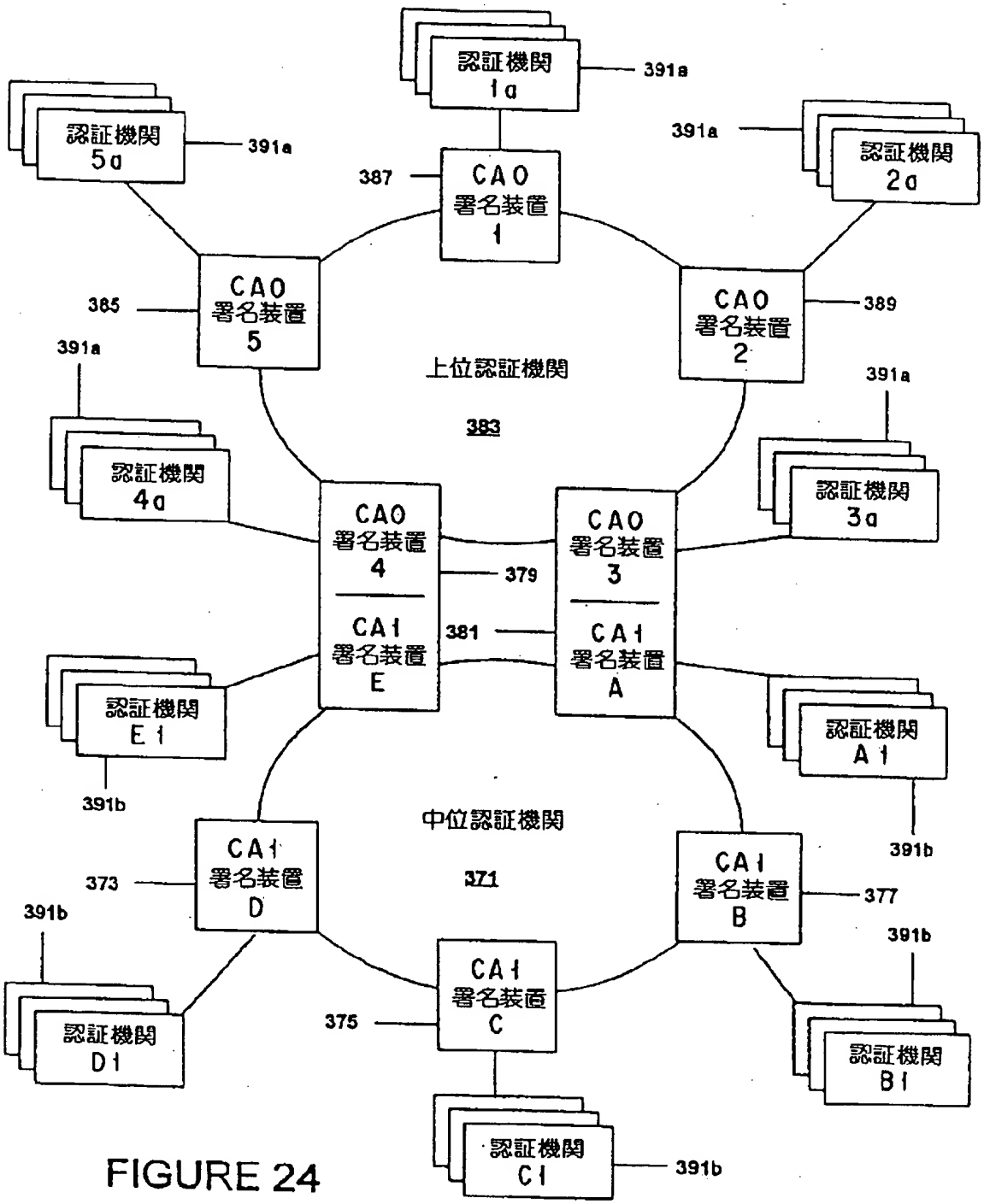


FIGURE 24

【図２５】

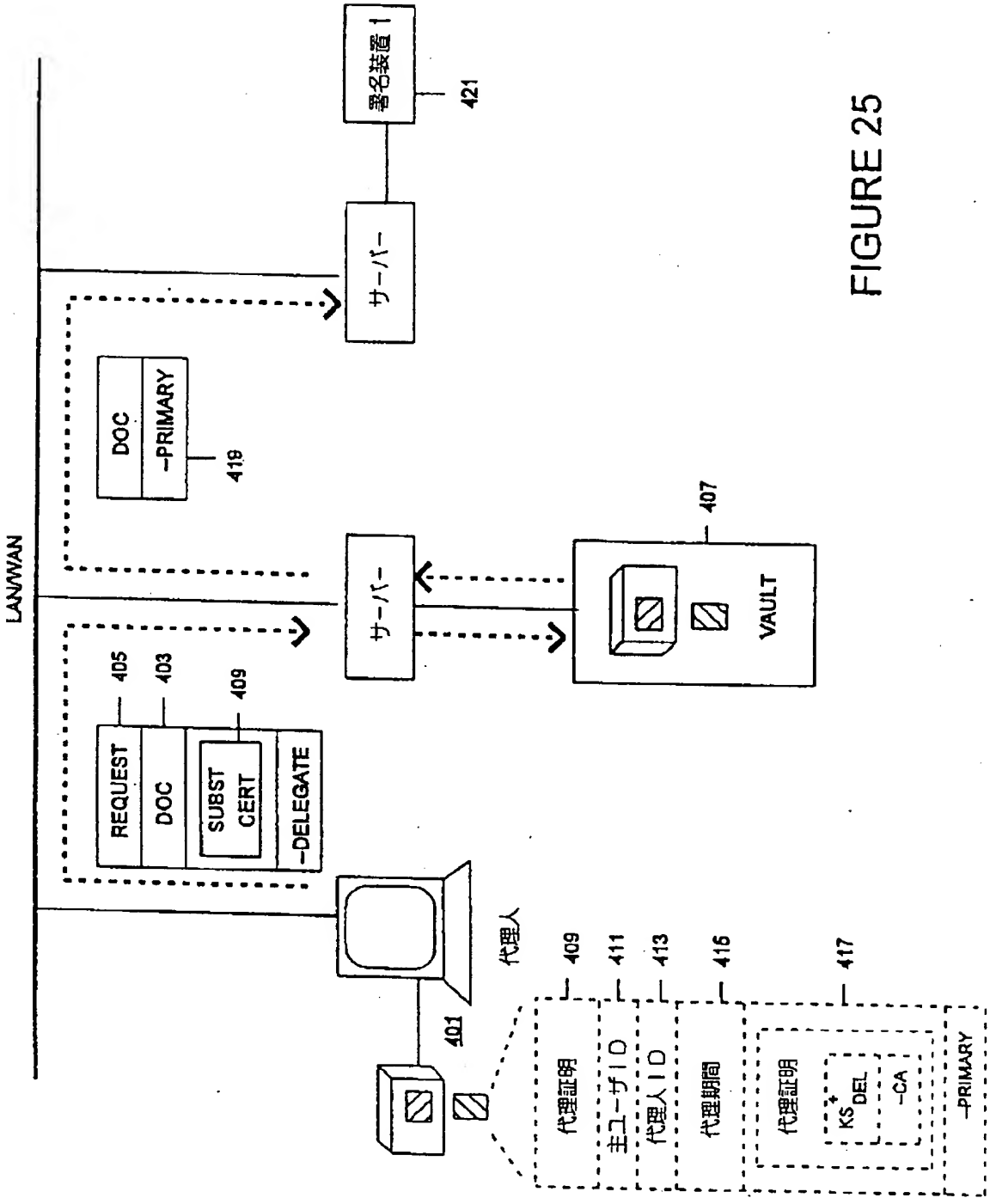


FIGURE 25

【手続補正書】特許法第１８４条の８第１項

【提出日】１９９７年２月４日

【補正内容】

プロセスを示す。

図６は署名装置を再認証するためのマルチステップ署名手順を示す。

図７は認証機関を認証し登録するためのシステム構造全体を示す。

図８は認証機関を使ったマルチステップ署名手順を示す。

図９は定型的なマルチステップ署名処理時に様々な認証機関や署名装置を通る文書の流れを示す。

図１０は定型的なマルチステップ署名処理時における文書に対する署名の進展を示す。

図１１はマルチステップ署名システムのパラレル実施例の文書の流れを示す。

図１２は３つの部分署名コピー、システムワイドオーソリティ署名への組み込み処理を示す。

図１３は認証機関の削除コマンドを示す。

図１４は認証機関の追加コマンドを示す。

図１５は製造者を追加するコマンドを伴う要求のサンプルを示す。

図１６は製造者を削除するコマンドを伴う要求のサンプルを示す。

図１７は型番号を追加するコマンドを伴う要求のサンプルを示す

図１８は型番号を削除するコマンドを伴う要求のサンプルを示す。

図１９は署名装置を追加するコマンドを含む命令のサンプルを示す。

図２０は署名装置を削除するメッセージを示す。

図２１Ａは送信装置にキー部分をコピーさせる要求のサンプルを示す。

図２１Ｂは送信装置から受信装置へのメッセージサンプルを示す。

図２２は格納しているキー部分を暗号化する処理を示す。

図２３は暗号化されたキー部分と、復号化キーのキー部分を生成し、分配する処理を示す。

図２４はインターロックリング機構を示す。

図２５は代理署名認証機関に代理証明書を発行する処理を示す。

発明を実施するための最良の形態

先ず、いくつかの計算プロセスから始めて、マルチステップ署名方法を最も直截に説明する。

A．順次部分署名における乗法方式

最初に、システム全体で有効な権限に属する公開／秘密鍵の対の秘密署名鍵K_{SAW}は、署名鍵K_{SWA}が部分の閾値ｔ０の積として計算できるように、部分a_iの数ｎ０として表される。ここで、ｔ０はｎ０に等しいか、それ以下である。このように表されるので、ｔ０より少ない部分を処理しても、署名鍵K_{SWA}を回復することは極めて困難である。例えば、これは以下の、１）Shamir式の秘密共用方式を使う、(A. Shamir, " How to Share a Secret", Communications of the ACM, Nov. 1979, V. 22, n.11)、２）Blakey式の秘密共用方式を使う(G. R. Blakley, "Safeguarding Cryptographic keys", Proceedings of the National Computer Conference, 1979, American Federation of Information Processing Societies, V.48, 1979, pp. 242-268)、３）鍵を因数分解する、４）既知の因数の積として鍵を作成することにより実行できる。必要なことは、秘密鍵が以下のように表わされることだけである。

$K_{SWA}=a_1*a_2*\ldots*a_{t0}(\mathrm{mod}\ 2N)$

ここで、K_{SWA}は、署名鍵であり、a_iはｔ０部分の組み合わせである。

第２に、各装置に前の装置が残した部分署名を累乗させることにより複数の装置を用いて、また秘密鍵の１つの部分を用いて、署名が作成される。法Ｎを使う場合（ここでは、演算は、法Ｎによって結果を割り、剰余を法Ｎの結果として取ることにより終る）、指数の乗算と順次累乗の間の以下の関係が真になる：

$(X^{a1*a2})(\mathrm{mod}\ N)=((X^{a1})^{a2})(\mathrm{mod}\ N)=((X^{a2})^{a1})(\mathrm{mod}\ N)$

言い換えれば、ベース値ｘが２つの因数ａ１とａ２の積によって累乗されると、ベースが最初の因数ａ１によって累乗され、その結果が２番目の因数ａ２によって累乗されたかのように、結果は同じになる。さらに、累乗の順序を反転することができる。それにより、最初にベースが２番目の因数ａ２によって累乗され

、その結果が最初の因数ａ１によって累乗されたのと同じ結果になる。この関係は、３以上の因数による累乗に一般化することができる。特に明記しない場合、すべての演算は、法Ｎと見なされなければならない。

マルチステップ署名方式では、署名鍵a_1, a_2, ..., a_{n0}の部分は別個の装置に配布される。最初の装置は、文書をハッシングし、以下のようなハッシュ(Hash)関数を累乗して文書に部分署名を添付する（記号Ｈは、ハッシュ演算の結果を示すのに使われている）。

最初の部分署名 = $(H)^{a1} (\mathrm{mod}\ N)$

２番目の装置は、以下のように２番目の部分a_2を用いて、最初の部分署名を累乗して追加署名を行なう。

２番目の部分署名 = $((H^{a1}))^{a2} (\mathrm{mod}\ N)$

ｔ０装置がそれぞれのｔ０部分を用いてハッシュを累乗し、公開鍵$\bar{K}_{SWA}$を用いて認証できる最終署名を作成するまで、このプロセスが繰り返される。

B．非同期的部分署名での加算方式

同じような結果を得るための代替方式では、署名権限者の秘密鍵を、法Ｎで加算して、秘密鍵を作成できるような部分に分割する。

$K = a_1 + a_2 + \ldots a_t (\mathrm{mod}\ N)$

これによって、以下に示すように、ハッシュを各部分で累乗しその結果を掛けて、別個に中間値$(H)^{ai}$を得て、非同期的にマルチステップ署名を実行することができるようになる。

$S = H^{a1} * H^{a2} * \ldots H^{a3} (\mathrm{mod}\ N)$

これは、メッセージをある位置から別の位置に順次ルーティングする必要がないので、先に説明した順次法よりも、処理面でかなり有利である。その代わりに、中央の管理者は、部分署名を求めて、同じメッセージ（または、ハッシュ）を直接に各位置に送り、その部分署名を結合して、最終の正式署名を作成することができる。部分署名にまだ含まれていない情報を追加することはないので、この最終結合処理は特別のセキュリティを必要としない。したがって、管理者はデスクトップから作業することができる。確かに、取り引きを検証する受領者が、部

分署名を後で結合するという作業を行わなければならないが、これにより正式署名のセキュリティが弱まることはない。

マルチステップ署名を行えるように変更できる累乗に基づいた署名方式には、以下のものがある。R. Rivest, A. Shamir and L. Adleman（ＲＳＡ）,「ディジタル署名と公開鍵暗号化システムを得るための方法」, Communications of the ACM, v.21, n.2, pp.120-126, February 1978); D. Kravitz, Digital Signature algorithm（ＤＳＡ）, U.S. Patent No. 5,231,668; Desmet, Y. Frankel,「閾値暗号化システム」, CRYPTO, '89, pp.307-15, 1989: Taher El-Gamal,「離散化アルゴリズムに基づいた公開鍵暗号化システムと署名方式」,（"El-Gamal Signature Alqorithm"）, IEEE Transaction on Information Theory, Vol. IT-31, No.4, Jul. 1985; S. Micali「安全で効率的なディジタル署名システム」, MIT／LCS／TM-501, Massachusetts Institute of Technology, laborator for Computer Science, March 1994; A. Menezes et al.,「楕円曲線公開鍵暗号化システム」, 1993。

システム概要

図１は、本発明に従った署名システムの構造の概要を示している。この構造は、広域ネットワーク（ＷＡＮ）またはローカルエリアネットワーク（ＬＡＮ）２１によって相互に接続された複数の署名装置１１，１３，１５，１７，１９を含んでいる。個々の署名装置１１，１３，１５，１７，１９は、ＷＡＮ／ＬＡＮが許す限り、地理的にいかなる範囲にでも分散させることができる（複数の大陸、複数の都市、１つの都市の複数の地域）。

図１には、署名装置２が、例として詳細に示されている。各署名装置には、通

られるコマンドは、ＭＤ５メッセージダイジェストを持ったＲＳＡ署名のように、標準（ＰＲＣ）の方式を用いて送り手により署名されると想定する。以下の図面では、装置暗号化／復号化鍵や装置署名／認証鍵が省かれることがあるが、これは、先に説明したように、すべての装置にあてはまると理解しなければならない。

図２は、安全なデータセンターコンピュータ構成４８の好ましい構造を示して

いる。ここには、図１の各署名装置が存在している。署名装置３９の他に、各データセンター構成４８は、さらに別個のメッセージサーバ４７を含んでいる。署名装置３９は、署名処理専用であり、金庫のような堅固な場所に位置している。署名装置と外部コンピュータネットワークの間は、直接接続されていない。以下で詳細に説明するように、署名装置３９は、マルチステップ署名３６のためのキー部分、自分自身の署名鍵３７、認証機関を識別するテーブル３８、キー部分３６に一致するように選ばれた公開鍵である公開認証鍵４０のための認証を提供される（ここでは、証明書はマルチステップ法を用いてフルKS_{SWA}によって署名される）。

マルチステップ署名プロセスでは、署名装置３９は、メッセージサーバ４７を介して要求を受け取る。メッセージサーバは、介在者が添付している通常のプライバシエンベロープを剥ぎ取ったり（サーバ４７は、署名装置のプライベート復号化鍵を処理しない）、処理速度を越えて提示された場合に行われる入力のキューイングのような通常のの通信プロセスを実行する。メッセージサーバは、署名のために署名装置にメッセージを提供し、署名（または部分署名）結果を受け取り、(a)部分署名結果を要求者に返すか、(b)結果をプロトコルの次の装置に渡す。通常の通信プロトコルを受け取り、そのプロトコルに参加するために、メッセージサーバは、暗号化したメッセージを受け取り、開くことができるように、自分自身のメッセージに署名するための公開／秘密鍵の対３２、３３を所有し、暗号化のための他の対３４、３５を所有する。これにより、安全な署名プロセスのセキュリティを大きく損うことなく、このルーチン負荷から署名装置を解放する。

メッセージサーバ４７は、通常の安全なデータセンタのような、セキュリティレベルの低い環境にある、比較的セキュリティレベルが低いコンピュータでも差

めのアプリケーションファームウェア４９を保存するための領域を含んでいる。必要な際の一時的記憶装置として、未使用メモリがワークエリア５４として提供される。また、マクロチップは、暗号化／復号化や署名プロセスの加速数値演算を実行するためのハードウェアを持つ専用数値演算アクセラレータユニットとし

ての暗号化ユニット４６をオプションで含んでいることもある。さらに、マイクロチップは、製造者によって初期設定され、タイムスタンピング署名に有用なオプションの信用タイムクロック４８を含んでいる。そのために、適切なバッテリ電源が必要である。さらに、マイクロチップには、暗号化／復号化プロセスで使われるオプションの乱数生成器５０を含んでいる。また、スマートカードは、乱数生成で使われる、マイクロチップに内蔵または外付けのダイオードのような図示されないオプションのノイズ源を持っていることもある。

図２に示した署名装置は、認証機関の信用装置と同じ設計のスマートカードであることもある。

ネットワーク上での装置は、以下のような一連の段階を経て初期化される。

１）暗号化鍵の配布

２）署名装置の一時認証

３）認証機関の一時認証

４）キー部分の配布

５）署名装置の再認証

６）認証機関の認証

それぞれを順に説明する。システム初期化の後に、高度な証明書やその他の文書に署名するために使われる通常の方法を説明し、その高度化やバリエーションを取り上げる。

暗号化鍵の配布

各署名装置および認証機関の各スマートカードは、先に述べた特徴に従ってのみ動作し、その製造者がプロテクトメモリに保存されている装置署名鍵の対と装置暗号化鍵の対を提供している、改ざんに強い装置であるという意味で、信用装置であると想定している。このような装置の製造者は、最低限、高価な改ざん作業が行わなければ、自分自身のまたはユーザの秘密鍵を漏らさないということを

証明しなければならない。また、各装置は、製造者が署名した電子証明書を持つ

３）先導装置は、他の各装置のファームウェアのハッシュを自分のハッシュと

比較し、他の装置が詐称者でないことがチェックされる。

ここで、すべての署名装置は、他の装置の公開暗号化鍵と署名認証鍵を受け取っている。以後のすべてのメッセージは、送り手の秘密署名鍵によって署名され、送信者の公開認証鍵を用いて受信者により確認されると、理解される。また、すべての通信は受信者の公開暗号化鍵を用いて暗号化され、受信者の秘密復号化鍵を用いて復号化されると理解される。

これらの追加署名鍵は、以下で説明するマルチステップ署名では使われないが、ネットワーク法人の間での定例通信の暗号化と署名のために、装置の身元の証明として使われる。身元とグループへの所属の証明は、実際のマルチステッププロトコルで使われるマスター鍵の作成と配布の際に非常に重要である。

署名装置の一時証明

図４は、新参の署名装置の一時証明を示している。このプロセスでは、装置の製造者により署名されている、あるいは署名されていない署名装置の公開鍵証明書は、一時管理者（管理者）６１が署名した証明書によって置き換えられる。通常、この管理者は、システムの初期化と管理者のパーソナルスマートカードを使った動作を担当するオペレータである。この一時証明は、マルチステップ署名のために署名鍵を作成する際に使われ、ターゲットグループに属する署名装置の間でのセキュリティレベルを高める。実際には、正しい手順の実行を保証するために一時管理者は複数の人間の立ち会いの下で作業し、一時証明は、完全なマスター鍵作成プロトコルを実行するのに必要な最低限の時間（せいぜい数分または数時間）の間だけ有効であると予想される。

一時証明は、以下のような手順で行われる。

１）一時管理者６１は、秘密署名鍵６３と対応する公開認証鍵６５を作成する。

２）一時管理者６１は、各署名装置１１，１３，１５，１７，１９に公開署名認証鍵６５を送る。

３）各署名装置１１，１３，１５，１７，１９は、秘密署名鍵６７，６９，７１，７３，７５と図示されない公開認証鍵を作成し、署名鍵証明要求を管理者６１に送る。署名鍵証明要求は、署名装置の名前、例えば装置シリアル番号及び／

名認証鍵。再証明されなければならない鍵は、元々プロトコルの開始時に装置によって作成され、最初は一時的に管理者によって証明されたのと同じ公開鍵である。この鍵は、この特定のＳＷＡ鍵の部分を扱う署名装置のファミリーに属していることの恒久的な証印になる。装置署名鍵とそれに関連する製造者証明書は、このプロセスにおいて変わらず、装置の起源とその特性の証拠として恒久的に保存される。

２）署名装置２は、そのＳＷＡ署名鍵部分９３を用いて部分ＳＷＡ署名を添付する。部分署名は、以下の２ステップで作成される。最初に、署名装置２は、ハッシングされていない証明書に認証面で関係付けられる切り詰められた文字列を作成するハッシュ関数（例えば、ＭＤ５、ＳＨＡ）を適用する。この文字列は、数値（大きな整数）として操作できる２進数として表される。次に、署名装置２は、ハッシュ文字列をそのＳＷＡ署名鍵部分で累乗して部分署名を作成する。すなわち、署名装置２は、以下の式に従って、部分署名になる数値を作成する。

$$--SD2 = (HASH(CERT))^{[KEY\ SHARE\ 2]}\ modulo\ N$$

本文においても、図面においても、署名ブロックを構成するビットの列は、通常、署名者の識別ラベルの前に長いダッシュを付けることによって示されることに注意すべきである。作成されたブロックは、通常、署名されるデータのブロックの下部に追加される。それ以外の場合も、文脈から明白である。

３）署名装置２は、部分署名が行われた証明書１０５を署名装置３に送る。

４）署名装置３は、既に適用されている部分署名--SD2累乗することによってシステムワイドオーソリティ署名を完成する。すなわち、署名装置３は、以下の式に従って、数値を計算する。

$$--SD3 = [--SD2]^{[KEY\ SHARE\ 3]}\ modulo\ N$$

$$= ((HASH)(CERT)exp\ KEY\ SHARE\ 2)exp\ KEY\ SHARE\ 3)$$

$$= --SWA$$

署名装置によって添付された部分署名を、監査証跡として文書に添付したままにしておくことも許される。この簡単な例では、部分署名は２つしか要求されなかったことに注意すべきである。

５）署名装置３は、署名した証明書１０７を署名装置１に戻す。戻された署名

装置１は、証明書のコピーを他の署名装置に配布し、他の署名装置がその署名を認証できるようにする。

この例では、署名装置２、３は、この順序で署名を添付した。数が最少数のｔ０を越えている限り署名装置のいかなる組み合わせでも、またいかなる順序でも署名し、同じ署名を作成することができる。

署名装置のフルシステムによって実行される以後の処理はＳＷＡ署名によって証明されている装置（例えば、以下で説明するように、許可提供者の装置）からの要求に対してのみ実行されることが望ましいので、再証明は重要である。署名装置自身は、他の署名装置に対する要求を行うことができる。この手順により、署名装置自身が、ここで定義するマルチステップ署名プロセスを用いて、システムワイドオーソリティ（ＳＷＡ）全体によって証明される最初の装置になる。

先の再証明プロセスの代替実施例においては、ターゲット装置のグループが、先導装置による初期鍵作成の前に自分の再証明要求（署名なしの証明書）を送付する。先導装置は、断片に分割し、鍵全体を消去する前に、ＳＷＡ秘密署名鍵を作成する時点でこの証明書に署名する。システムの主要な機能は高度に統制され、しかも効率的内やり方でかかる証明書に署名しなければならないので、こうしたやり方には特別の利点は存在しないように思われる。

認証機関の再証明

図７と図８は、認証機関を証明し、登録するステップを示している。図７は、全体的なシステム構造を示し、図８は、証明要求の処理手順を示している。署名装置は、システムワイドオーソリティの正式署名を認証機関の証明書に添付し、各認証機関の公開署名認証鍵を証明する。登録プロセスにおいては、各署名装置は、署名装置にその部分署名を適用するように指示する力を持っている特定の認証機関の内部保存テーブルを更新する。ルーチンの処理時に、署名装置は、以下で詳細に説明するように、要求が最低数の一時証明またはＳＷＡ証明されている認証機関によって署名されている場合、または最低数の個別署名メッセージを受け取った場合にのみ、その部分署名を添付する。認証機関３ａ（ＡＡ３ａ）を証明し、署名装置３にＡＡ３ａを登録するプロセスは、以下のように進行する。

説明のために、署名装置３と１（図７の参照数字１５、１１）は、ＳＷＡ署名

を添付するために選ばれた５つの署名装置の内の２つであると想定している。

１）認証機関３ａ（１０９）は、ＬＡＮ／ＷＡＮ ２１を通じて、署名装置３に再証明要求を送付する（図８の参照数字１２１）。あるいは、許可及び／又は登録を、アクセス制限の設定されている通信チャネルを通した署名装置への直接接続に、例えばスタンドアロンコンピュータへの直接接続に制限することができる。証明要求には、少なくとも以下の情報が含まれている；ａ）認証機関の名前（人間の識別名）、ｂ）認証機関の信用装置の識別コード（例えば、スマートカードのシリアル番号や型番号）、ｃ）認証機関（人間）の署名認証鍵。これは装置が既知のタイプに属することの保証となる。すべてのまたは実質上すべての処理は広く分散した位置から実行され、システムオペレータは目視検査によっては何も認証できないので、このような保証は特に重要である。

２）署名装置３（１５）は、パーシャルＳＷＡ署名（－ＳＤ３）を証明書１２１に添付し、部分署名証明書１２３を他の認証機関に送る。

３）認証機関１ａは、部分証明書１２３をＳＤＩ（１０、１１）に送れるようにする。

４）署名装置１は、ＳＷＡ署名鍵の部分９３を用いて署名プロセスを完了する。

５）署名装置１は、署名が完成した証明書１２７を認証装置３ａに戻す。

６）署名装置１は、署名された証明書１２７のコピーを保存し、認証機関（図示しない）のログにＡＡ３ａと入力し、署名された証明書１２７を認証機関３ａに戻す。

署名装置３に登録されなければならないすべての認証機関に対してこのプロセスが繰り返され、各認証機関には署名付きの証明書を残し、署名装置３にはすべての証明書のログを残す。他の署名装置１１，１３，１７，１９のすべての認証機関に対して、このプロセスが繰り返される。

マルチステップ署名

この段階で、署名装置は、ＳＷＡ秘密署名鍵の部分によって初期化されている。署名装置は、自分自身を再証明しており、認証機関はその各署名装置で再証明、登録されている。ここで、システムは、システム管理と正式証明機能の両方の

ためのルーチンサービスに入る準備ができている。以下の説明では、通常システム

管理に使われるシステムワイドオーソリティキーについて、マルチステップ署名を説明する。以下で説明するように、追加のマスター鍵も、同じ装置ファミリー

２）ＡＡ１ｂの署名鍵を使ったハッシュの累乗。ＡＡ１ａの署名は、監査証跡として文書に残される。次に、ＡＡ１ｂは、新しいヘッダを添付し、２度署名された文書１３９を署名装置１に送る（図９の参照数字１１１）。

４）署名装置１は、２度署名された文書１３９を受け取り、ヘッダーを抜き取って、文書がその登録済み認証機関の署名を必要な数だけ、この例では２を持っているかどうかチェックする。持っている場合、署名装置１は認証機関の署名を抜き取って、部分ＳＷＡ署名を添付する。図１０に示すように、部分ＳＷＡ署名（--SD1）は、認証機関の署名のない基本文書をハッシングし、署名装置１のＳＷＡ署名鍵部分９３を用いてハッシュを累乗する。次に、署名装置１は新しいヘッダを添付し、部分署名文書１４１を別の署名装置の認証機関、ここでは、署名装置２の認証機関２ａに送る。

５）認証機関２ａ（図９の参照数字１４３）は、ヘッダを抜取り、いくつかの手順チェック（マルチステップ署名とは密接な関係はない）を実行して、文書に署名すべきかどうか判断する。証明書に署名すべきと判断すると、認証機関２ａは文書に署名する。図１０に示すように、ＡＡ２ａの署名（--AA2a）は、以下のものによって決められる。１）証明書と部分ＳＷＡ署名（--SD1）の連結組み合わせのハッシング、ｂ）ＡＡ２ａの再証明済み署名鍵を使ったハッシュの累乗。ＳＤ１の部分ＳＷＡ署名は、文書に残される。次に、ＡＡ２ａは、新しいヘッダを添付し、署名入りの文書１４５を認証機関２ｂに送る（図９の参照数字１４７）。

６）認証機関２ｂ（図９の参照数字１４７）は、ヘッダを抜取り、いくつかの手順チェック（マルチステップ署名とは密接な関係はない）を実行して、文書に署名すべきかどうか決める。文書に署名すべきであると判断すると、認証機関２

ｂは文書に署名する。図１０に示すように、ＡＡ２ｂの署名（--AA2b）は、以下のものによって決められる、１）証明書、部分ＳＷＡ署名、ＡＡ２ａの署名の連結組み合わせのハッシング、ｂ）ＡＡ２ｂの再証明済み署名鍵を使ったハッシュの累乗。部分ＳＷＡ署名とＡＡ２ａの署名は文書に残される。次に、ＡＡ２ｂは、新しいヘッダを添付し、署名入りの文書１４９を署名装置２に送る（図９の参照数字１３）。

る。例では、ユーザを（再）証明し（再）登録するには、人間による４つの署名だけが必要であることに注意。

パラレル署名

図１１は、マルチステップ署名システムのパラレル実施時における文書の流れを示している。この図では、システムには総数３の署名装置１６９ａ，１６９ｂ，１６９ｃがあり、システムワイドオーソリティ（ＳＷＡ）署名を完成するにはこれら３つの署名装置が必要であると想定している。パラレル署名は、これとは異なる数の署名装置に適合しうると理解されなければならない。

パラレル法では、文書統合器１６１（コーディネータ）は、署名すべき文書１６３を受け取る。しかし、統合器はいずれかの署名装置の認証機関である必要はないが、統合器は通常、別個の法人として図示される。

文書統合器１６１は、署名すべき文書１６３の３つのコピー１６５ａ，１６５ｂ，１６５ｃ（または、文書のハッシュの３つのコピー）を作成する。各コピーは、最初の認証機関１６７ａ，１６７ｂ，１６７ｃに送られ、次に２番目の認証機関１７１ａ，１７１ｂ，１７１ｃに送られ、次に３つの署名装置１６９ａ，１６９ｂ，１６９ｃのいずれかに送られた後、最後に統合器１６１に戻される。以下で詳細に説明するように、文書統合器は、３つの署名装置の署名を結合し、署名入り文書１７３を作成するために元の文書１６３に添付されるシステムワイドオーソリティ署名（--SWA）を作成する。

図１２は、いずれかのコピーの処理および３つの部分署名のシステムワイドオーソリティ署名への組み込みを示している。各コピーは基本的に同じ処理をされると理解しなければならない。しかし、それぞれの認証機関と署名装置はその個

別署名鍵に応じて署名または部分署名を添付するという例外がある。

この例では、各署名装置１６９ａがその署名を添付できるようにするには、２つの認証機関が必要である。統合器１６１は、自分の署名（--AA1a）を添付し、２度署名された署名入りコピー１７５ａを２番目の認証機関１７１ａに送る最初の認証機関１６７ａに対するルーティング情報ヘッダ（図示されない）と共に、署名する文書の最初のコピー１６５ａを送る。２番目の認証機関１７１ａは、２番目の許可署名を添付し、２度署名された文書１７９ａを署名装置に送

る。署名装置１６９ａは、２つの許可署名を認証し、部分署名（--SD1）をコピーに添付して、署名入りコピー１８１ａを統合器１６１に戻す。

図示されない他の２つの署名装置は、署名される文書のコピーに部分署名を添付し、署名入りコピー１８１ｂ，１８１ｃを統合器に戻す。これら３つのコピーは、パラレルに処理することができる。

統合器が署名すべき文書のコピー３つ１８１ａ，１８１ｂ，１８１ｃをすべて受け取った後、統合器は、３つの部分署名（--SD1，--SD2，--SD3）を掛け合わせる。３つの部分署名の積が、システムワイドオーソリティ署名（--SWA）になる。

認証機関の署名装置とスマートカードは、信用装置である。このパラレルマルチステップ署名法のセキュリティは、統合器のワークステーションの物理的セキュリティには依存していない。統合器は、認証機関に許可を与えるために、いかなる秘密鍵も処理する必要はない。しかし、通常、プライバシや識別のためにルーティング暗号化鍵および署名鍵を持っている。

統合器の機能を認証機関の間に配分することもできる。最初の認証機関は、署名すべき最初の文書を受け取り、部分署名を受け取り結合する別の認証機関を指定することもできる。あるいは、いずれかの署名装置のサーバのような認証機関でない別の法人でも指定できる。組織の通常、の運営では統合器に署名すべき文書を受け取ってもらい、署名入り文書の最後の受領者への配送を担当してもらうのが望ましいと思われる。

認証機関の追加／削除

各署名装置は、認証機関の関連グループを持っている。人が組織を出入りするので、システムは、認証機関の信用装置の公開鍵を追加および削除することによって、許可提供者を動的に追加または削除するための決まりを持っている。認証機関の追加または削除は、認証機関の公開鍵の追加や削除を行うコマンドの署名装置への送付によって行われる。コマンドは、追加／削除コマンドのコード、追加情報（以下で説明する）、そして許可署名を持っている電子メッセージの形を取る。

許可署名は、同じ署名装置の他の認証機関から来ることもあり、追加／削除の

名付き電子要求を送付することによって削除することができる。図１８は、コマンド２７３、製造者の名前２７５、型番号２７７を含む要求のサンプル２７１を示している。

署名装置の追加／削除

次第に、システムに署名装置を追加したり、システムから署名装置を削除しなければならなくなる。各署名装置は、ＳＷＡ鍵の部分、または、以下で詳細に説明するマルチステップ署名のための他のマスター鍵の部分、システム上の他の署名装置のテーブルを含んでいる。各署名装置の身元は、以下によって定義される、１）装置識別番号（例えば、シリアル番号）、２）製造者によってインストールされ、製造者の署名の下で証明される鍵、あるいはＳＷＡ署名が再証明する同じような鍵である装置公開認証鍵、３）暗号化メッセージを装置に送るために使われる装置公開暗号化鍵、４）以後所有するユニークな証明済み公開鍵。

新しい署名装置は、ＳＷＡ署名を受け取るために他の装置の間に署名なしの証明書を回覧してから、署名入り証明書を回覧することによって、システムに追加される。証明書には、先に述べたように、識別情報が含まれる。ＳＷＡ鍵によって証明書が署名された後、証明書は、新しい装置を他の署名装置の内部テーブルに追加する指示と共に、すべての他の署名装置に送られる。図１９は、コマンド２８３と証明書２８２を含んでいる指示のサンプル２８１を示している。証明書は、新しい署名装置ＩＤコード２８５、製造者が署名した署名装置の署名認証鍵証明書２８７、やはり装置製造者が署名している署名装置の暗号化鍵証明書２８

９を含んでいる、。署名認証鍵と暗号化鍵が１つの証明書に入っていることもある。新しい署名装置が使うキー部分２９１や新しい装置に預けられる暗号化鍵２９２の部分のような他の情報を他の署名装置の間で回覧しなければならない。署名装置をグループに追加すると、以下のことが可能である、１）新しいマスター鍵を作成し、その部分を受け取るためにプロトコルに参加する、２）署名ＳＤの内容を受け取るバックアップユニットとして動作する、または３）破壊されたあるいはサービスから除かれたリビジョンバックアップ署名装置の復旧内容を受け取る代替ユニットとして動作する。

図２０は、署名装置を取り除くためのメッセージ２９３を示している。メッセ

全な、例えば、金庫室に保管された、そしてオフラインのリモート攻撃を受けることがない記憶装置にコピーすることができる。

過半数要件の変更

ＳＷＡ鍵を添付するのに使われる署名装置の過半数は、キー部分作成時に先導装置によって使われるシステム設計パラメータである。この過半数は、署名鍵全体を回復するためにキー部分を結合し直し、後で元のキー部分と同様に再配布される、新しい過半数要件を持った、より多数の部分に鍵を分割することによって変更することができる。

特定の署名装置が部分署名を添付できるようにするのに必要な認証機関の過半数は、システムを初期化し直さなくても変更可能である。この変更は、各署名装置にＳＷＡ鍵によって署名された要求を送付することによって実行するのが望ましい。あるいは、特定の署名装置の認証機関は、ローカル認証機関だけが署名した要求を送付することによってローカル過半数を変更できる。過半数を変えるのに必要な署名の数は、署名装置がＳＷＡ署名を添付することができるようにするのに必要な数と同じであることも、また異なっていることもある。ＳＷＡキー部分が署名装置内に暗号化した形で保存されており、許可提供者が以下で説明するように復号化キー部分を持っている場合、署名に権限を附与するのに必要な過半数は、ＳＷＡキー部分を復号化するのに必要な部分の数より少なくしてはならない。通常、の銀行業務では、いくつかの許可提供者は複数の署名装置で権限を持

っていることがあるが、許可提供者Ｎは、署名装置毎に２より少なくてはならない。

保存されてるキー部分の暗号化

図２２に示すように、ここでは、１つの署名装置３２１内に保存されている各ＳＷＡキー部分は、暗号化した形３２３で保存されている。復号化鍵（ＫＥＹ）は、部分に分割されており、各認証機関の信用装置３２５，３２７，３２９が復号化鍵の部分を保存している。先に説明したように、署名装置が部分署名を添付するようにという各要求は、過半数の認証機関の署名によって実行されなければならない。この場合、認証機関はさらに復号化鍵３３１，３３３，３３５の部分を署名装置３２１に送る。次に、署名装置は以下のことを行う。

るようにという、ＳＷＡ署名鍵が署名した電子メッセージを送付することによって、他の署名装置から回復でき、新しく登録されたすマートカードにインストールし直すことができる。あるいは、ＳＷＡの同意があれば、受け取り権限を持っている者の信用装置の公開暗号化鍵の下で暗号化するようにして、ある装置がすべての復号化鍵を受け取り、その署名部分を復号化し、新しい暗号化キーペアを作成し、公開鍵の下で署名部分を再度暗号化し、新しい秘密復号化鍵を新しい部分に分割し、この部分を関連の認証機関の信用装置に再配布するようにすることができる。

また、バックアップ法を使えば、復号化キー部分は、米国特許出願第０８／１８１，８５９号と第０８／２７７，４３８号で説明されているように、独立した信託機関にオフラインで保管することができる。

暗号化ハートビート

さらなる防衛策として、各署名装置は、中断された場合に、署名装置が非活性化される定期的データ入力（ハートビート）を受け取るということもある。ハートビートは、署名装置から離れた位置で作成されるので、誰かが署名装置を盗もうとしても、その者はハードビートの発生源を手に入れるために隔離した部屋または地下室に進入しなければならない。ハートビートの発生源を手に入れることができない場合、署名装置は非活性になっているので、何の役にも立たない。

各署名装置がハートビート発生源に暗号化鍵を提供するという実施例もある。ハートビート発生源は、定期的に暗号化したメッセージを署名装置に送る。署名装置が、ハートビート発生源から一定時間の間に最低数のメッセージを受け取ることができない場合、署名装置はその内部メモリを消去するか、他の回避行動を取る。メッセージは空のメッセージや単純なメッセージでよいが、ＳＤによって与えられた公開キーを用いて、ハートビート発生源が暗号化しなければならない。あるいは、メッセージは、疑似乱数発生器（ＲＮＧ）がハートビート発生源で作成し、署名装置の同期乱数発生器（ＲＮＧ）が認証した疑似乱数文字列でも差し支えない。

署名装置が一定時間の間に少なくとも１つ（あるいは最低数）の発生源からメッセージを受け取れるように、複数のハートビート発生源を設置することができ

請求の範囲

１．秘密署名鍵の部分を作成するステップと、

別個の電子署名装置へ部分を保存するステップと、

署名装置の複数の認証機関を認証するステップと、

複数の署名装置のそれぞれにおいて、最低数の認証機関からの認証に応じて電子メッセージに部分署名を添付するステップとを具備し、

複数の部分署名によってディジタル署名が構成されるディジタル署名方法。

２．ディジタル署名を電子文書に添付するシステムであって、

電子文書を受け取り、予め決められた数の認証に応じて、署名鍵部分を用いて部分署名を添付するようにプログラミングされている電子装置からなる複数の相互通信署名装置と、

関連の署名装置と通信でき、関連の署名装置に認証を提供するようにプログラミングされている電子装置からなる複数の認証機関とを具備するシステム。

３．電子文書にディジタル署名を添付するための署名装置のインターロックリングシステムであって、

複数の電子装置を含んでおり、それぞれの装置は、電子文書を受け取り、最初の署名鍵に部分署名を添付するようにプログラミングされ、この複数の部分署名

は最初のディジタル署名を含んでいる、署名装置の第１集合と、

複数の電子装置を具備し、各装置は、電子文書を受け取り、第２署名鍵のために部分署名を添付するようにプログラミングされ、この複数の部分署名は２番目のディジタル署名を含んでいる、署名装置の第２集合とを具備し、

前記署名装置の第１集合は、前記第２集合には含まれないメンバーを少なくとも１つは含み、第１集合と第２集合は少なくとも１つの共通メンバーを含むシステム。

５．前記複数の署名装置は、

メッセージを複数の署名装置の中の第１の署名装置に送信し、第１の署名装置が前記メッセージに第１の部分署名を添付するステップと、

前記第１の部分署名が添付されたメッセージを複数の署名装置の中の第２の署名装置に送信し、第２の署名装置が前記メッセージに第２の部分署名を添付する

ステップとからなる方法に従って多数の部分署名をメッセージに添付する請求の範囲第１項記載の方法。

６．前記送信ステップは前記複数の署名装置の数だけ繰り返される請求の範囲第５項記載の方法。

７．前記複数の署名装置は秘密署名鍵の部分を格納している署名装置の過半数である請求の範囲第６項記載の方法。

８．前記前記ディジタル署名を形成するに必要な署名装置の過半数は変更され、同一の秘密署名鍵は、

秘密署名鍵を形成するために各署名装置からの部分を再結合するステップと、

ディジタル署名を形成するために必要な部分の過半数が必要に応じて変更できるように秘密署名鍵の新部分を発生するステップと、

別個の電子署名装置に新部分を格納するステップとからなる方法に従って秘密署名鍵の部分を再分配することにより保たれる請求の範囲第７項記載の方法。

９．前記過半数はディジタル署名を形成するために必要な部分署名の数を増加することにより変更できる請求の範囲第８項記載の方法。

１０．前記過半数は署名装置の数を増加することにより変更できる請求の範囲

第９項記載の方法。

１１．前記複数の認証機関は前記別個の電子署名装置の少なくとも１つに割り当てられ、

前記電子署名装置が前記部分署名を添付するためには前記複数の認証機関の過半数からの認証が必要である請求の範囲第１項記載の方法。

１２．前記複数の署名装置は、

メッセージを複数の署名装置の各々に送信し、各々の署名装置が部分署名を伴った複数のメッセージを形成するために前記複数の署名装置の各々において前記メッセージに部分署名を添付するステップと、

ディジタル署名を持ったメッセージを形成するために前記部分署名を伴った複数のメッセージを結合するステップとからなる方法に従って多数の部分署名をメッセージに添付する請求の範囲第１項記載の方法。

１３．前記複数の署名装置は秘密署名鍵の部分を格納している署名装置の過半数である請求の範囲第１２項記載の方法。

１４．前記複数の署名装置は、

メッセージを複数の署名装置の中の第１の署名装置に送信し、前記メッセージに第１の部分署名を添付するステップと、

前記第１の部分署名が添付されたメッセージを複数の署名装置の中の第２の署名装置に送信し、前記メッセージに第２の部分署名を添付するステップとからなる方法に従って多数の部分署名をメッセージに添付する請求の範囲第２項記載の方法。

１５．前記送信ステップは前記複数の署名装置の数だけ繰り返される請求の範囲第１４項記載の方法。

１６．前記複数の署名装置は秘密署名鍵の部分を格納する署名装置の過半数である請求の範囲第１４項記載の方法。

１７．前記複数の署名装置は

メッセージを複数の署名装置の各々に送信し、部分署名を伴った複数のメッセージを形成するために前記複数の署名装置の各々において前記メッセージに部分

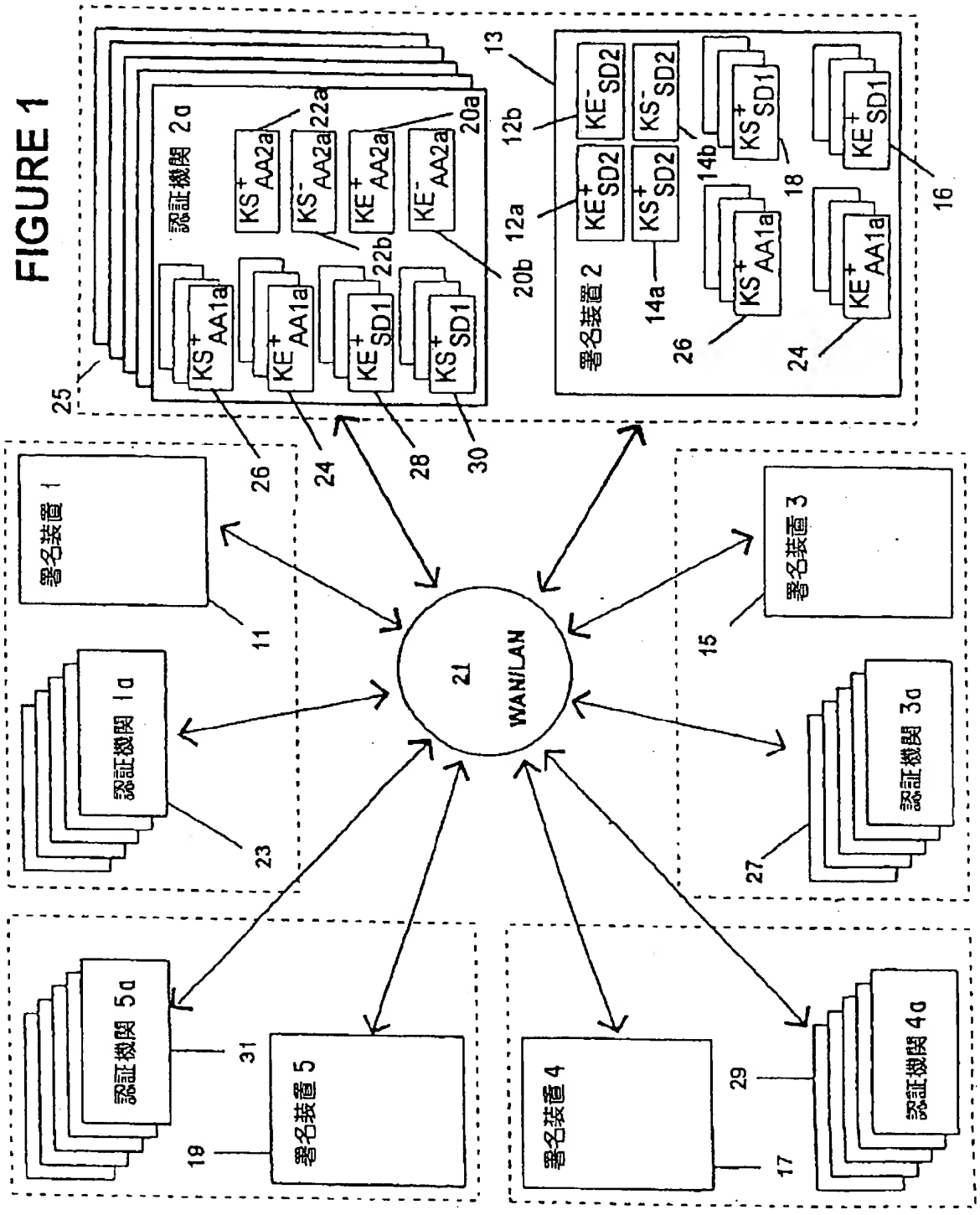
署名を添付するステップと、

ディジタル署名を持ったメッセージを形成するために前記部分署名を伴った複数のメッセージを結合するステップとからなる方法に従って多数の部分署名をメッセージに添付する請求の範囲第２項記載の方法。

１８．前記複数の署名装置は秘密署名鍵の部分を格納する署名装置の過半数である請求の範囲第１７項記載の方法。

【図１】

FIGURE 1


署名装置 1
11
認証機関 1a
23
署名装置 2
認証機関 2a
25
署名装置 3
15
認証機関 3a
27
署名装置 4
17
認証機関 4a
29
署名装置 5
19
認証機関 5a
31
WAN/LAN
21
13
12a
12b
14a
14b
16
18
20a
20b
22a
22b
24
26
28
30

【図２】

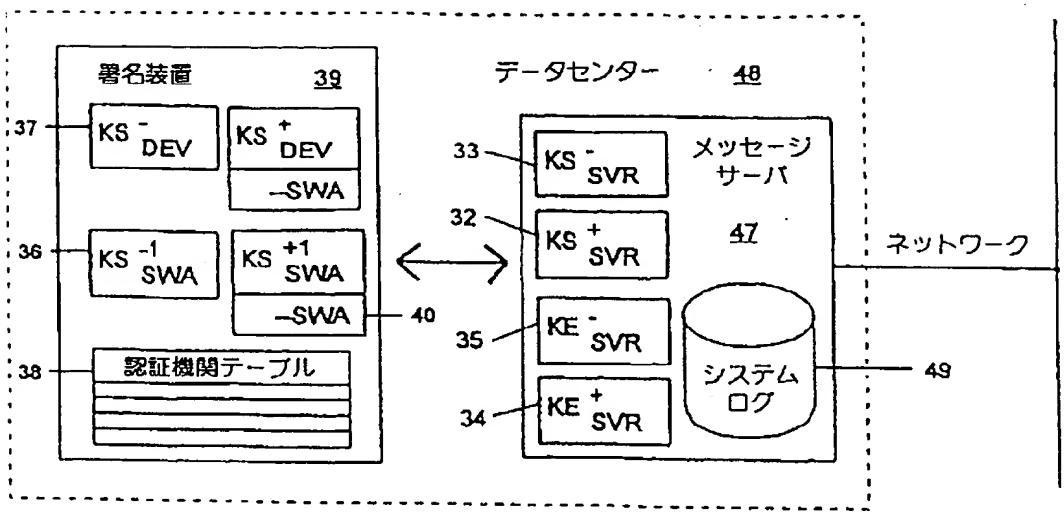


FIGURE 2

【図３】

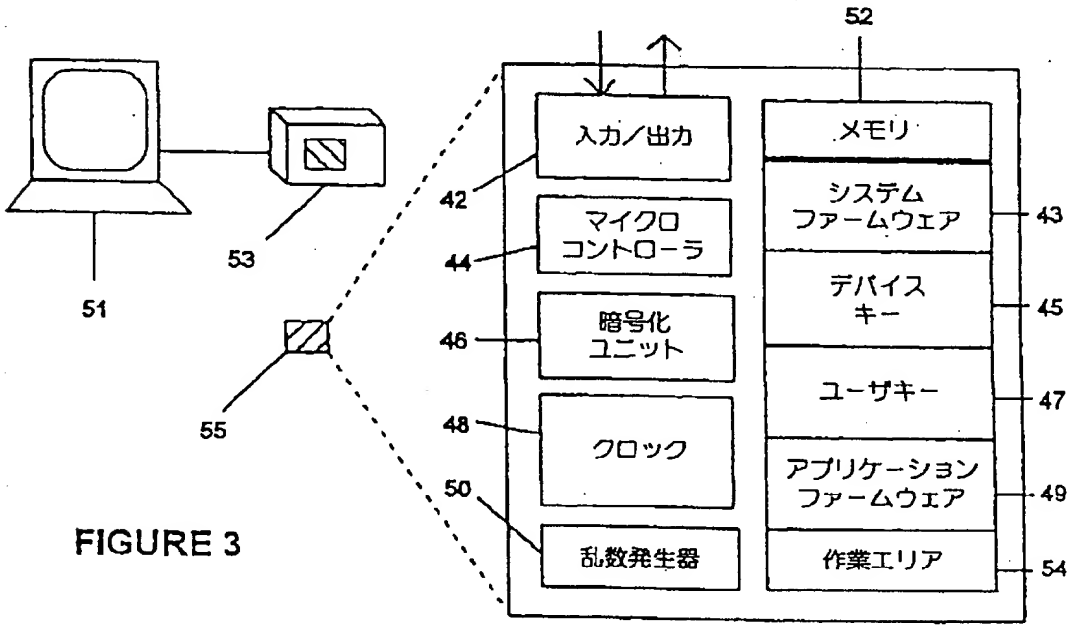


FIGURE 3

【図５】

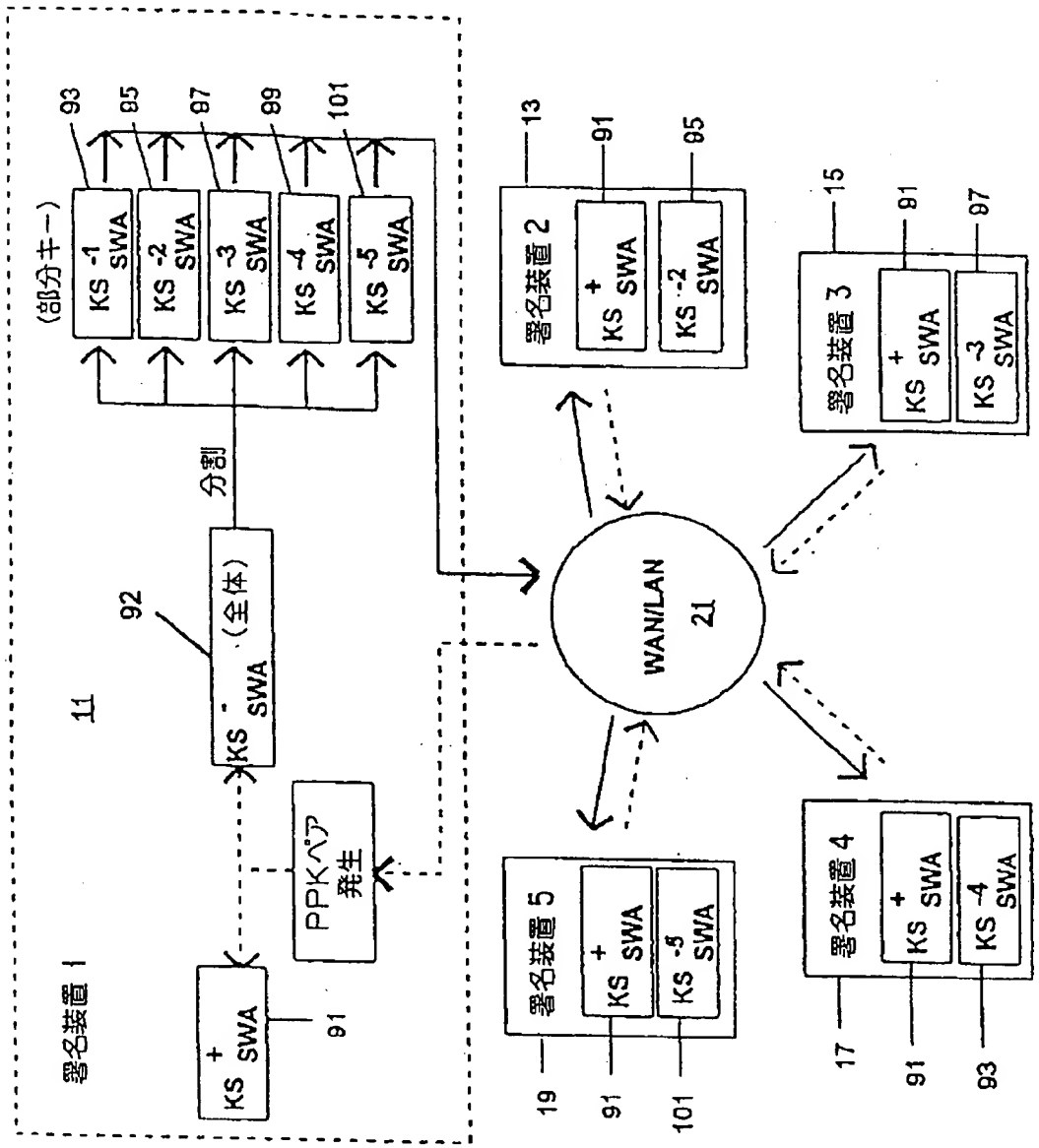

署名装置 1
11
(部分キー)
KS -1 SWA
KS -2 SWA
KS -3 SWA
KS -4 SWA
KS -5 SWA
93
85
87
89
101
分割
92
KS - SWA (全体)
PPKペア 発生
KS + SWA
91
WAN/LAN 21
署名装置 2
KS + SWA
KS -2 SWA
13
91
85
署名装置 3
KS + SWA
KS -3 SWA
15
91
97
署名装置 4
KS + SWA
KS -4 SWA
17
91
93
署名装置 5
KS + SWA
KS -5 SWA
19
91
101

FIGURE 5

【図８】

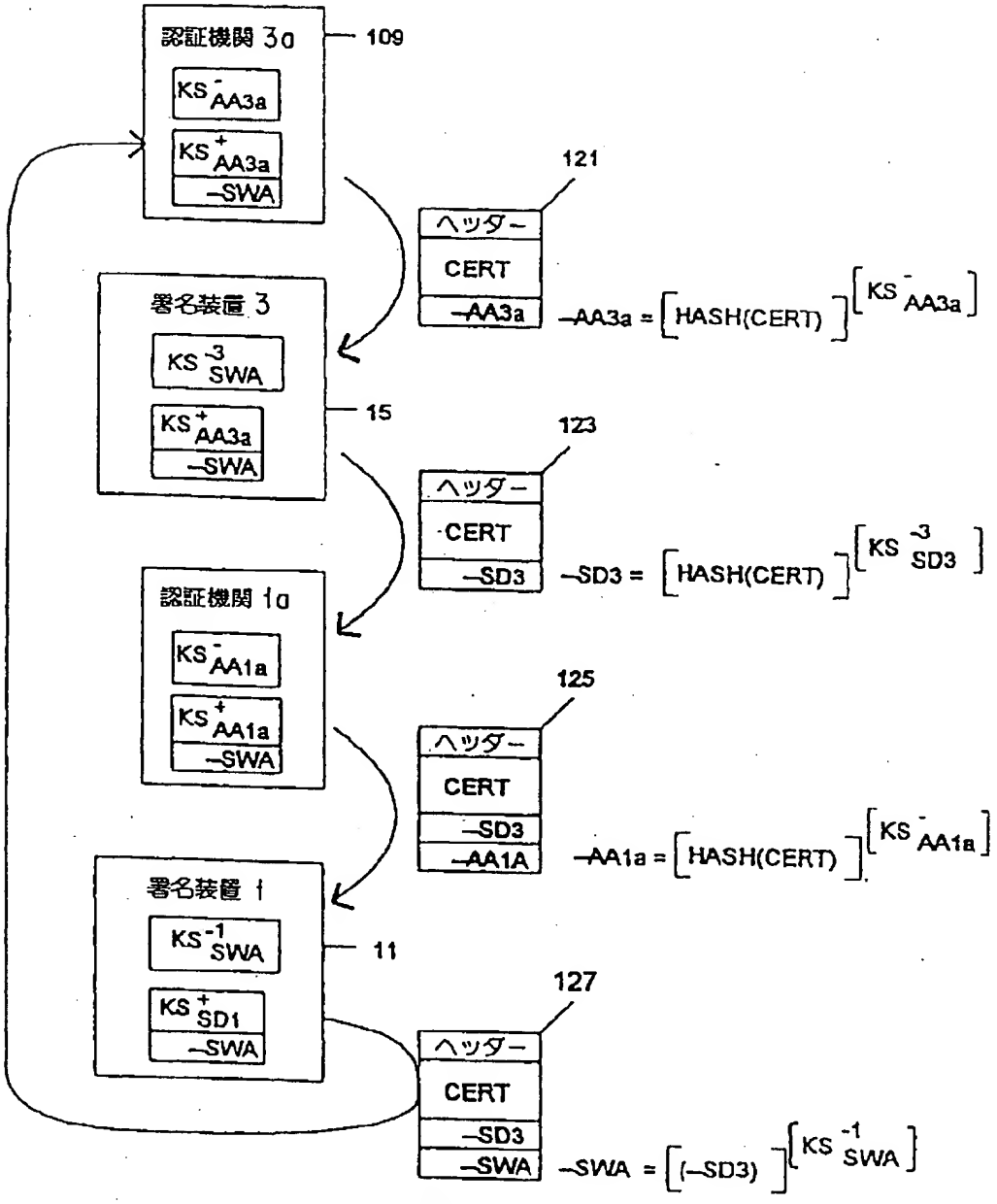

認証機関 3o
109
KS -AA3a
KS +AA3a
–SWA
121
ヘッダー
CERT
–AA3a
–AA3a = [HASH(CERT)] [KS -AA3a]
署名装置 3
KS -3SWA
KS +AA3a
–SWA
15
123
ヘッダー
CERT
–SD3
–SD3 = [HASH(CERT)] [KS -3SD3]
認証機関 1o
KS -AA1a
KS +AA1a
–SWA
125
ヘッダー
CERT
–SD3
–AA1A
–AA1a = [HASH(CERT)] [KS -AA1a]
署名装置 1
KS -1SWA
KS +SD1
–SWA
11
127
ヘッダー
CERT
–SD3
–SWA
–SWA = [(–SD3)] [KS -1SWA]

FIGURE 8

【図９】

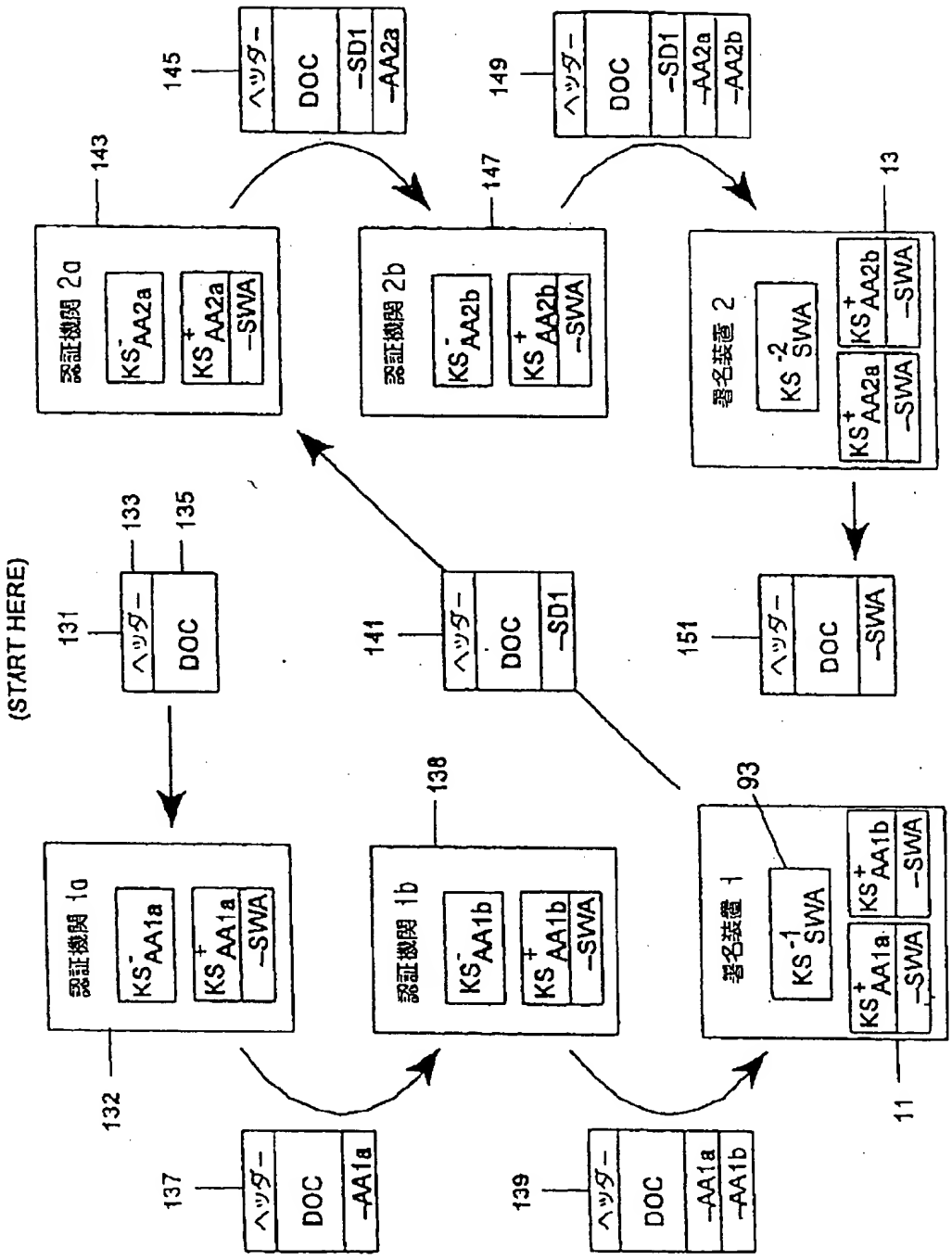

(START HERE)
131
133
135
141
151
145
149
143
147
13
132
138
93
11
137
139
ヘッダー
DOC
-SD1
-AA2a
-AA2b
-SWA
-AA1a
-AA1b
認証機関 2a
認証機関 2b
署名装置 2
認証機関 1a
認証機関 1b
署名装置 1

FIGURE 9

【図１９】

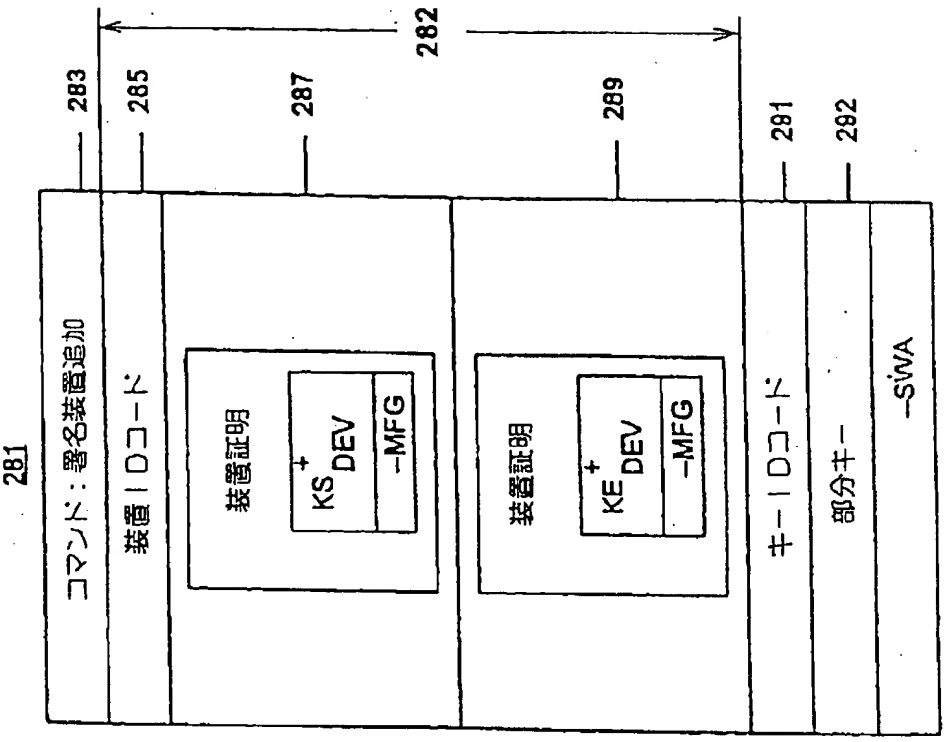


FIGURE 19

【図２０】

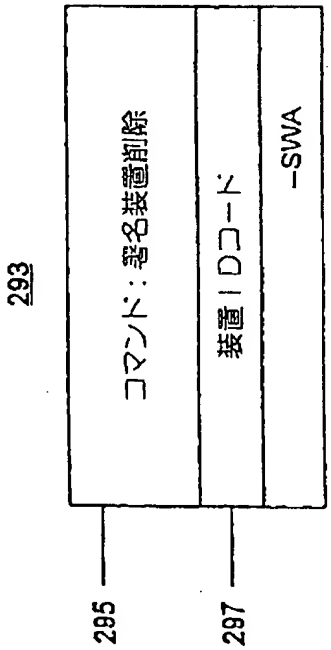


FIGURE 20

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US96/05317

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :H04L 9/30, 9/32
US CL :380/23, 30
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 380/23, 30

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US, A, 5,276,737 (MICALI) 04 JANUARY 1994, col. 2, lines 41-62.	1, 2
Y, P	US, A, 5,481,613 (FORD ET AL) 02 JANUARY 1996, col. 8, line 53 through col. 9, line 1.	1, 2
A	US, A, 5,005,200 (FISCHER) 02 APRIL 1991, col. 11, line 4 through col. 12, line 62.	3
Y	US, A, 5,224,163 (GASSER ET AL) 29 JUNE 1993, col. 15, line 8 through col. 16, line 8.	4
A	US, A, 5,164,988 (MATYAS ET AL) 17 NOVEMBER 1992, col. 19, lines 21-67.	4

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 07 AUGUST 1996	Date of mailing of the international search report 25 OCT 1996
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer GILBERTO BARRÓN JR. Telephone No. (703) 306-4177

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

Inter...ional application No.
PCT/US96/05317

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Please See Extra Sheet.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US96/05317

BOX II. OBSERVATIONS WHERE UNITY OF INVENTION WAS LACKING
This ISA found multiple inventions as follows:

This application contains the following inventions or groups of inventions which are not so linked as to form a single inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fees must be paid.

Group I, claim(s) 1 and 2, drawn to a method and system of digital signing with a plurality of signing devices and a plurality of authorizing agents.
Group II, claim(s) 3, drawn to a system of interlocked rings of signing devices.
Group III, claim(s) 4, drawn to an electronic method for delegating use of an electronic key.The inventions listed as Groups I, II and III do not relate to a single inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons:
Groups II and III lack the special technical feature of a plurality of signing devices and a plurality of authorizing agents of Group I.
Group III lacks the special technical feature of interlocked rings of signing devices of Group II.
Groups I and II lack the special technical feature of an electronic method for delegating use of an electronic key of Group III.

フロントページの続き

(81)指定国 EP(AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AP(KE, LS, MW, SD, SZ, UG), UA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN

(72)発明者 ファン、スチュアート・ティー・エフ
アメリカ合衆国、ワシントン、ディーシー 20008、エヌ・ダブリュ・ナンバー 907、バン・ネス・ストリート 2939